**PART III**

**(Pages 101-150)**

**Publication No. EP 0950968**

**Dated: 02-1999**

**(English Publication of WO 9909502 corresponding to Korean Publication No. 2000-0068758)**

**(Previously filed in IDS of December 5, 2007)**

[0953] When the electronic payment card is purchased or transferred, the card status 2007 for the electronic payment card is in the disabled state. To set the card status 2007 to the enabled state, the electronic payment card must be registered in the service providing system 110.

[0954] When the service providing system 110 separately manages an electronic payment card to be used and an electronic payment card that is unused and is in the sleeping state, the operating cost of the electronic payment card service is reduced, and the illegal use of the electronic payment card is prevented by changing, during the registration process, the digital signature keys for the electronic payment card.

[0955] When the electronic payment card is registered, the card status 2007 represents the enabled state. The card signature private key 2010 is changed to a new card signature private key, and accordingly, the card certificate 2003 is changed to the registered card certificate 2033. Further, in the service providing system 110, the electronic payment card is registered in the service director information server 901 as an electronic payment card that is to be used by the user who registered the payment card.

[0956] Fig. 21 is a specific diagram showing the data structure of an electronic telephone card 2100. In Fig. 21, the electronic telephone card 2100 consists of three portions: a telephone card program, a presentation card and a card certificate portion. The telephone card program portion is information for managing the status of a telephone card and for specifying an operation inherent to a telephone card. The presentation telephone card portion is information that is to be presented to the electronic telephone card accounting machine 800 of the switching center 105 as information for the contents of a telephone card when a call is made using an electronic telephone card. The card certificate is issued by a service provider for an electronic telephone card, and indicates that the electronic telephone card is authentic. There are two types of card certificates: a card certificate 2103 for simply certifying an electronic telephone card, and a registered card certificate 2133 for certifying that an electronic telephone card is registered in the service providing system. The card certificate 2003 can be changed to the registered card certificate 2032 when the user registers an electronic payment card.

[0957] One electronic telephone card, as well as one electronic ticket or one electronic payment card, includes three key types and four different keys in accordance with the public key cryptography method. One key type is a key used for a digital signature accompanying an electronic telephone card, and a card signature private key 2110 and a card signature public key 2125 (2136) are provided as a private key and a corresponding public key. Another key type is a card private key 2111 used for the electronic telephone card authorization process performed with the electronic telephone card accounting machine 800 of the switching center 105. The other key type is an accounting machine public key 2112 used for the authorization process for the electronic telephone card accounting machine 800 performed by the mobile user terminal 100.

[0958] The card signature private key 2110 and the card signature public key 2125 (2136) are a key pair that differs for each electronic telephone card. The card private key 2111 and the accounting machine public key 2112 differ for each telephone card type. The electronic telephone card accounting machine 800 of the switching center 105 includes a card public key and an accounting machine private key that correspond to the card private key 2111 and the accounting machine public key 2112. The method for employing these keys will be described in detail later.

[0959] In Fig. 21, first, the telephone card program 2101 includes ten items of information: telephone card program header 2104, card name 2105, card ID 2106, card status 2107, total remaining value 2108, micro-check issuing number 2109, card signature private key 2110, card private key 2111, accounting machine public key 2112 and telephone card program data 2113 information.

[0960] The card program header 2104 is header information indicating that the entry is a telephone card program and describing the data structure of the telephone card program. The card name 2105 and the card ID 2106 are the name and the ID of an electronic telephone card. The card ID is identification information that differs for each electronic telephone card.

[0961] The card status 2107 is information describing the status of an electronic telephone card, concerning whether the electronic telephone card can be used, whether it is unused, whether it has been registered, and whether it can be transferred.

[0962] A remaining card amount 2108 is information providing the remaining amount that is held by the

electronic telephone card.

[0963] The micro-check issuing number 2109 is the issue number for a micro-check that is issued by an electronic telephone card, and is incremented each time a telephone micro-check is issued. For each electronic telephone card, an arbitrary number is set as the initial number that is employed as the micro-check issuing number. The initial number is managed by the service providing system 110, and is employed as verification data in the micro-check reference process. The micro-check reference process will be described in detail later.

[0964] The card signature private key 2110 is a digital signature private key for the electronic telephone card 2100. Similarly, the card private key 2111 is used for the authorization process for the electronic telephone card 2100, and the accounting machine public key 2112 is used for the authorization process for the electronic telephone card accounting machine 800 of the switching center 105.

[0965] The card signature private key 2110 is used, in the telephone card clearing process and the telephone card transfer process, to provide a digital signature for data consisting of the card status 2107 and the total remaining value 2108 for the electronic telephone card 2100 in the electronic telephone card accounting machine 800 or the mobile user terminal to which the electronic telephone card is transferred.

[0966] The telephone card program data 2113 is a program module for specifying an operation inherent to the electronic telephone card.

[0967] The program module for specifying a common operation for the electronic telephone card is stored in the ROM 1501. The basic operations, such as the exchange of messages with the electronic telephone card accounting machine 800 of the switching center 105 to call a micro-check, the generation of messages to be exchanged and the updating of the card status 2107, and the standard format for the display of an electronic telephone card on the LCD 303, are defined by the program module that is stored in the ROM 1501.

[0968] The card program data 2113 is a program module for specifying the operations inherent to the telephone card clearing process and inherent to the display process. The card program data 2113 consists of three data sets: a transaction module set 2130, a representation module set 2131 and a representative component information set 2132.

[0969] The transaction module 2130 is a program module for specifying an operation inherent to the telephone card settlement processing. Since the transaction module 2130 is specified, in the telephone card settlement processing, messages can be exchanged among the procedures that differ from normal, or inherent information can be included in a message to be exchanged.

[0970] The transaction module 2130 does not have to be specified if this is not required. When the transaction module 2130 is not defined, it acts as an electronic telephone card for the performance of the basic telephone card clearing process.

[0971] The representation module 2131 is a program module for specifying an operation on the display, such as a location on the LCD 303, data to be displayed and a display form. The representation module 2131 also does not have to be defined if such is not necessary. When the representation module 2131 is not defined, an electronic telephone card is displayed in the standard display format.

[0972] The representative component information 2132 is image information comprising a component of a telephone card on the display, such as an illustration, a photo, a map or a background image. The representative component information 2132 does not have to be specified if such is not necessary. When the representative component information 2132 is not specified, the electronic telephone card is displayed using only with text information, as is shown in Fig. 3E. When the representative component information 2132 is specified, the electronic telephone card is displayed using the standard display format. When the representation module 2131 is specified, the image information included in the representative component information is displayed as an image 315 in accordance with the representation module 2131, as is shown in Fig. 3H.

[0973] The design of an electronic telephone card having a high degree of freedom can be specified by a combination consisting of the transaction module 2030, the representation module 2131 and the representative component information 2132.

[0974] The presentation card 2102 includes eight information items: a presentation card header 2114, a card code 2115, a card ID 2116, card information 2117, a telephone card issuer ID 2118, a validity term 2120, a service provider ID 2121, and a card issuing date 2122. A digital signature is provided for the card ID 2116, the card information 2117 and the card issuer ID 2118 by the card issuer (2119), and a digital signature is provided for the presentation card 2102 by the service provider.

[0975] The presentation card header 2114 is header information indicating that the pertinent card is a presentation card and indicating the data structure of the presentation card. The card code 2115 is code information indicating an electronic telephone card type. And the card ID 2116 is ID information for an electronic telephone card, and is the same information as that given for the card ID 2106.

[0976] The card information 2117 is ASCII information that indicates the contents of a telephone card. In the card information 2117, a face value of a telephone card when it is issued, usage condition information, an issuer, and information as to whether an electronic telephone card can be transferred, are described using a form to which tag information are added to represent the individual information types. When the standard display format or the representation module 2131 is designated, the card information 2117 is displayed on the LCD 303 in accordance with the representation module 2131, as is shown in Fig. 3E or 3H.

[0977] The card issuer ID 2118 is ID information that identifies the telephone card issuer who issued the pertinent telephone card. The validity term 2120 is information concerning the period the electronic telephone card 2100 is valid. The service provider ID 2121 is ID information for the service provider. And the telephone card issuing date 2122 is information concerning the date on which the service provider issued the electronic telephone card 2100.

[0978] The card certificate 2103 and the registered card certificate 2133 have substantially the same data structure.

[0979] The card certificate 2103 includes seven information items: a card certificate header 2123, a card ID 2124, a card signature public key 2125, a card certificate ID 2126, a certificate validity term 2127, a service provider ID 2128, and a card certificate issuing date 2129. A digital signature is provided for the card certificate 2103 by the service provider.

[0980] The card certificate header 2123 is header information labeling this as a card certificate and describing the data structure of the card certificate. The card ID 2124 is ID information for the electronic telephone card 2100, and is the same information as that provided by the card ID 2106 and the card ID 2116.

[0981] The card signature public key 2125 is a public key that is paired with the card signature private key 2110 for use as the digital signature for the electronic telephone card 2100. The card certificate ID 2126 is ID information for the card certificate 2103. The certificate validity term 2127 is information indicating the period during which the card certificate 2103 is valid. The service provider ID 2128 is ID information for identifying the service provider who issued the card certificate 2103. The card certificate issuing date 2129 is information providing the date on which the card certificate 2103 was issued.

[0982] The registered card certificate 2133 includes seven information items: a registered card certificate header 2134, a card ID 2135, a card signature public key 2136, a card certificate ID 2137, a certificate validity term 2138, a service provider ID 2139, and a card certificate issuing date 2140. A digital signature is provided for the registered card certificate 2133 by the service provider.

[0983] The registered card certificate header 2134 is header information labeling this as a registered card certificate and describing the data structure of the registered card certificate. The card ID 2135 is ID information for the electronic telephone card 2100, and is the same information as that provided by the card ID 2106 and the card ID 2116.

[0984] The card signature public key 2136 is a public key that is paired with the card signature private key 2110 for use as the digital signature for the electronic telephone card 2100. The paired card signature private key 2110 and card signature public key 2136 have greater lengths and provide greater security than do the paired card signature private key 2110 and card signature public key 2125.

[0985] In the telephone card registration process, the paired card signature private key 2110 and card signature public key 2125 used as the digital signature for the electronic telephone card are updated to the new, more secure paired card signature private key 2110 and card signature public key 2136.

[0986] The card certificate ID 2137 is ID information for the registered card certificate 2133. The certificate validity term 2138 is information concerning the term during which the registered card certificate 2133 is valid. The service provider ID 2139 is ID information identifying the service provider who issued the registered card certificate 2133. The card certificate issuing date 2140 is information concerning the date on which the registered card certificate 2133 was issued.

[0987] The card certificate does not constitute information for certifying the electronic telephone card 2000, but instead constitutes information with which the service provider certifies the card signature public key 2125 (or the card signature public key 2136). The card certificate is added to the telephone micro-check accompanied by the digital signature for which the card signature private key 2110 is used, so that the legality of the micro-check can be verified.

[0988] When the electronic telephone card is purchased or transferred, the card status 2107 for the electronic telephone card is in the disabled state. To set the card status 2107 to the enabled state, the electronic telephone card must be registered in the service providing system 110.

[0989] When the service providing system 110 separately manages an electronic telephone card to be used and an electronic telephone card that is unused and is in the sleeping state, the operating cost of the electronic telephone card service is reduced, and the illegal use of the electronic telephone card is prevented by changing, during the registration process, the digital signature keys for the electronic telephone card.

[0990] When the electronic telephone card is registered, the card status 2107 represents the enabled state. The card signature private key 2110 is changed to a new card signature private key, and accordingly, the card certificate 2103 is changed to the registered card certificate 2133. Further, in the service providing system 110, the electronic telephone card is registered in the service director information server 901 as an electronic telephone card that is to be used by the user who registered the telephone card.

[0991] As is described above, the electronic ticket 1900, the electronic payment card 2000 and the electronic telephone card 2100 have similar data structures. Especially, the electronic payment card and the electronic telephone card have basically the same data structure, so that an electronic payment card that has the functions of both an electronic payment card and an electronic telephone card can be implemented. In this case, in the payment card settlement processing and in the telephone card settlement processing, the price of a product and a communication charge are subtracted from the remaining card amount held by one electronic payment card.

[0992] Further, when information that corresponds to the remaining card amount 2008 held by the electronic payment card 2000 and the remaining card amount 2108 held by the electronic telephone card 2100 is set as a part of the variable ticket information 1908 provided for the electronic ticket 1900, a coupon ticket can be implemented that functions as a ticket, a payment card and a telephone card. This is especially effective for a travel coupon ticket in which are packaged an overseas travel ticket, a shopping ticket and a portable telephone usage right.

[0993] The internal structure of the gate terminal 101 will now be described.

[0994] Fig. 22 is a block diagram illustrating the arrangement of the gate terminal 101. The gate terminal 101 comprises: a CPU (Central Processing Unit) 2200, which processes data for transmission and reception, in accordance with a program stored in a ROM (Read Only Memory) 2201, and which controls the other components via a bus 2242; a RAM (Random Access Memory) 2202 and a hard disk 2203 on which are stored data that are to be processed and data that have been processed by the CPU 2200; a EEPROM (Electric Erasable Programmable Read Only Memory) 2204, in which are stored the gate ID of the gate terminal 101, the terminal ID and a telephone number for a telephone terminal, a merchant ID, a private key and a public key for the digital signature of a merchant, the service provider ID and the telephone number of the service providing system (the telephone number of the service provider is accompanied by the digital signature of the service provider), and the public key of the service provider; a cryptographic processor 2205, which encrypts or decrypts data under the control of the CPU 2200; a data codec 2206, which encodes data to be transmitted and decodes received data under the control of the CPU

2200; a touch panel LCD 401, which displays an image set up by the CPU 2200, and detects touch manipulation effected by a merchant; an infrared communication module 400, which provides infrared communication with the mobile user terminal 100; a serial port 2209, which is connected to the infrared communication module 400; a serial-parallel converter 2208, which performs the bidirectional conversion of parallel data and serial data; a key operator 2212, which detects a merchant's manipulation of a lock switch 405, a menu switch 404, a number key switch 403 and a power switch 402; a loudspeaker 2211, through which sounds are output to provide notification concerning the completion of the ticket examination process and the establishment of the operation; a sound controller 2210, which drives the loudspeaker 2211; a digital telephone communication unit 2207, which provides digital telephone communication with the service providing system 110 via the digital telephone communication line 120; an external interface 2213, which is an interface for the connection of an external device, such as a gate opening/closing device; and a control logic unit 2214, which processes an interrupt signal received from the key operator 2212, the touch panel LCD 401, the serial-parallel converter 2208, the digital telephone communication unit 2207 and the external interface 2213, and which serves as an interface when the CPU 2200 accesses an internal register of the key operator 2213, the touch panel LCD 401 or the sound controller 2210.

[0995] The cryptographic processor 2205 includes a secret key encryption and decryption function and a public key encryption and decryption function. The cryptographic processor 2205 employs a cryptography method determined by the CPU 2200 and the keys for the encrypting or decrypting of data set by the CPU 2200. The CPU 2200 employs the encrypting and decrypting functions of the cryptographic processor 2205 to perform a digital signature process or a closing process for a message, and to decrypt a closed and encrypted message or to verify a digital signature accompanying a message. A detailed explanation will be given later for the digital signature process, the closing process, the decryption process and the digital signature verification process.

[0996] The data codec 2206 encodes data to be transmitted or decodes received data under the control of the CPU 2200. In this case, the encoding is a process for the generation of data to be transmitted that includes communication control information and error correction information, and the decoding is a process for the performance of error correction for the received data and the removal of extra communication control information in order to obtain the data that a sender was to originally transmit. The data codec 2206 has a function for encoding or decoding data during data communication via a digital telephone, and a function for encoding or decoding data during infrared communication. The data codec 2206 performs encoding or decoding as determined by the CPU for data that are set by the CPU.

[0997] When, for example, a closed message accompanied by a digital signature is to be transmitted via digital telephone communication, the CPU 2200 employs the cryptographic processor 2205 to perform a digital signature process and a closing process for the message, employs the data codec 2206 to encode the obtained message to obtain a data communication form for a digital telephone, and transmits the resultant message through the control logic unit 2214 to the digital telephone communication unit 2207.

[0998] When a closed message accompanied by a digital signature is to be received via digital telephone communication, the CPU 2200 receives that message from the digital telephone communication unit 2207 through the control logic unit 2214, employs the data codec 2206 to decode the received message, and permits the cryptographic processor 2205 to decrypt the closed and encrypted message and to verify the digital Signature accompanying the message.

[0999] Similarly, when a closed message accompanied by a digital signature is to be transmitted via infrared communication, the CPU 2200 employs the cryptographic processor 2205 to provide a digital signature for the message and to close the message, and employs the data codec 2206 to encode the obtained message to provide a data form that is suitable for infrared communication. Then, the resultant message is transmitted through the control logic unit 2214 to the serial-parallel converter 2208.

[1000] When a closed message accompanied by a digital signature is to be received via infrared communication, the CPU 2200 receives that message from the serial-parallel converter 2208 through the control logic unit 2214, employs the data codec 2206 to decode the received message, and permits the cryptographic processor 2205 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1001] When the merchant depresses either the lock switch 405, the menu switch 404, the number key switch 403, or the power switch 402, the key operator 2212 asserts, to the CPU 2200, an interrupt signal 2237 requesting the performance of a process corresponding to the manipulation of the switch. As is shown

in Fig. 23A, the key operator 2212 includes a key control register (KEYCTL) 2306 for setting the valid/invalid state of each switch. And to set the valid/invalid state of each switch, The CPU 2200 accesses the key control register (KEYCTL) 2306.

[1002] As is shown in Fig. 23A, the touch panel LCD 401 includes an X coordinate register (XCOORD) 2304 and a Y coordinate register (YCOORD) 2305, which correspond to the coordinates of the point on the screen that the merchant touches. When the merchant touches the screen, the touch panel LCD 401 asserts an interrupt signal 2235 requesting the performance of a process corresponding to the manipulation of a switch. In response to the interrupt, the CPU 2200 reads the coordinate information from the X coordinate register (XCOORD) 2304 and the Y coordinate register (YCOORD) 2305 via the control logic unit 2214, and performs a process based on the coordinate information.

[1003] The sound controller 2210, as is shown in Fig. 23A, includes an audio processor control register (SCTL) 2303, for controlling the audio processing, that the CPU 2200 accesses To control the operation of the sound controller 2210. When, for example, the ticket examination process has been normally completed, the CPU 2200 accesses the audio processor control register (SCTL) 2303 to output a sound signalling that the ticket has been examined. Thus, the sound controller 2210 drives the loudspeaker 2211, through which is output the sound signalling that the ticket has been examined.

[1004] The infrared communication module 400 modulates a serial digital signal that is received via the serial cable 406 to obtain a signal that is actually to be transmitted as an infrared ray, and further changes the resultant signal to an infrared ray and emits it. Furthermore, the infrared communication module 400 changes a received infrared ray to an analog signal, and then demodulates the analog signal to obtain a digital signal and outputs it.

[1005] To transmit a message by using infrared communication, the CPU 2200 transmits the message as a digital signal 2226 to the serial-parallel converter 2208 via the control logic unit 2214. The serial-parallel converter 2208 converts the message into a serial digital signal, and transmits it via the serial port 2209 and the serial cable 406 to the infrared communication module 400, which then outputs the infrared ray.

[1006] When the infrared ray is received by the infrared communication module 400, the serial digital signal received at the infrared communication module 4300 is transmitted via the serial cable 406 and the serial port 2209 to the serial-parallel converter 2208, whereat the signal is converted into parallel data. At this time, the serial-parallel converter 2208 asserts the interrupt signal 2227 and requests that the CPU 2200 process the received data.

[1007] The digital telephone communication unit 2207 controls digital telephone communication with the service providing system 110 via the digital telephone communication line 120. As is shown in Fig. 23A, the digital telephone communication unit 2207 includes an ID register (ID) 2307, in which the terminal ID of the gate terminal 101 is stored, and a digital telephone communication unit control register (TCTL) 2308, which controls the operation of the digital telephone communication unit 2207.

[1008] The digital telephone communication unit 2207 converts data that are to be transmitted via digital telephone communication into a data format for digital telephone communication, and transmits the resultant data to the digital telephone communication line 120. The data are transmitted to the control logic unit 2214 by the CPU 2200 as a digital signal 2223.

[1009] In response to a call received along the digital telephone communication line 120, the digital telephone communication unit 2207 examines the terminal ID and receives and decodes the data. At this time, the digital telephone communication unit 2207 further asserts an interrupt signal 2224 requesting that the CPU 2200 process the received data.

[1010] The external interface 2213 is an interface circuit for connecting an external device, such as a gate opening/closing device. The CPU 2200 controls the external device via the control logic unit 2214 and the external interface 2213. A control signal 2245 is employed for the writing and reading operations performed by the CPU 2200 via the control logic unit 2214. At a low level, the control signal signifies a writing operation, while at a high level, the control signal signifies a reading operation. A data signal that is exchanged at this time by the control logic unit 2214 and the external interface 2213 is a digital signal 2243, and an interrupt signal 2244 is a control signal that is issued as an interrupt request by the external device.

[1011] The control logic unit 2214, as is shown in Fig. 23A, includes three internal registers: a clock counter

(CLOCKC) 2300, an update time register (UPTIME) 2301, and an interrupt register (INT) 2302.

[1012] The clock counter is employed to measure the current time; the update time register is employed to store the time at which the gate terminal 101 will communicate with the service providing system to update data in the RAM 2202 and on the hard disk 2203; and the interrupt register is employed to indicate the reason an interrupt is generated for the CPU 2200.

[1013] When the count held by the clock counter 2300 matches the count in the update time register 2301, or when one of the interrupt signals 2224, 2227, 2235, 2237 or 2244 is asserted, the control logic unit 2214 writes the reason for the interrupt in the interrupt register (INT) 2302, and asserts an interrupt signal 2222 requesting the CPU perform an interrupt process. For the interrupt processing, the CPU 2200 reads the reason stored in the interrupt register and then performs a corresponding process.

[1014] The individual bit fields of the interrupt register (INT) are defined as is shown in Fig. 23B.

[1015] Bit 31 represents the state of the power switch. When the bit value is 0, it indicates the state is the power-OFF state, and when the bit value is 1, it indicates the state is the power-ON state.

[1016] Bit 30 represents the digital telephone communication state. When the bit value is 1, it indicates the state is one wherein digital telephone communication is in process.

[1017] Bit 29 represents the generation of a touch panel interrupt due to contact being made with the touch panel. When the bit value is 1, it indicates that touch panel interrupt has occurred. In this bit field, a 1 is set when the interrupt signal 2235 is asserted.

[1018] Bit 28 represents the generation of an infrared ray reception interrupt. When the bit value is 1, it indicates that an infrared ray has been received. In this bit field, a 1 is set when the infrared communication module 400 receives an infrared ray and the interrupt signal 2227 is asserted.

[1019] Bit 27 represents the generation of a data reception interrupt. When the bit value is 1, it indicates that data is being received. In this bit field, a 1 is set when the data-communication data are received and the interrupt signal 2224 is asserted during the course of digital telephone communication.

[1020] Bit 26 represents the generation of an update interrupt requesting the performance of a data updating process. When the bit value is 1, it indicates the generation of the update interrupt. In this bit field, a 1 is set when the count in the clock counter matches the count in the update time register.

[1021] Bit 25 represents the generation of an external IF interrupt requesting data communication be initiated with the external device that is connected to the external interface 2213. When the bit value is 1, it signals the generation of the external IF interrupt. In this bit field, a 1 is set when the interrupt signal 2244 received from the external interface 2213 is asserted.

[1022] Bit 24 represents the generation of a key interrupt by the manipulation of the switch. When the bit value is 1, it represents the generation of the key interrupt. In this bit field, a 1 is set when the interrupt signal 2237 is asserted.

[1023] Bits 0 to 9 correspond to switches 0 to 9 for the number key switches. Bit 10 and bit 11 correspond to number key switches "*" and "#" and bits 12 to 15 correspond to function switches F1 to F4. Bits 16 to 18 respectively correspond to the power switch, the lock switch, and the menu switch. When the bit value is 1, it indicates that a switch corresponding to that bit has been depressed.

[1024] Data stored in the RAM 2202 will now be described.

[1025] Fig. 24 is a specific diagram showing a RAM map for data stored in the RAM 2202.

[1026] The RAM 2202 is constituted by five areas: a fundamental program objects area 2400, a service data area 2401, a merchant area 2402, a work area 2403, and a temporary area 2404. In the fundamental program objects area 2400 are stored an upgraded module for a program stored in the ROM 2201, a patch program, and an additional program. The merchant area 2402 is an area that a merchant can freely use, the work area 2403 is a work area that the CPU 100 employs when executing a program, and the temporary area 2404 is an area in which information received by the gate terminal is stored temporarily.

[1027] The service data area 2401 is an area in which is stored contract information for the electronic commerce service, information for an electronic ticket to be examined and history information, and the data in this area are managed by the service providing system 110. The service data area 2401 is constituted by seven sub-areas: a data management information area 2405, a merchant information area 2406, a merchant public key certificate area 2407, a merchant preference area 2408, a ticket list area 2409, a transaction list area 2410 and an authorization report list area 2411.

[1028] The data management information area 2405 is an area in which is held management information for data stored in the service data area 2401; the merchant information area 2406 is an area in which is stored the name of a merchant and information concerning the contents of a contract entered into with the service provider; the merchant's public key certificate area 2407 is an area in which is stored a public key certificate for the merchant; a merchant preference area 2408 is an area in which is stored for a merchant preference information that concerns an electronic ticket service; the ticket list area 2409 is an area in which is stored list information for electronic tickets that the gate terminal examines; the transaction list area 2410 is an area in which is stored history information for the ticket examination process of the electronic ticket service; and the authorization report list area 2411 is an area in which are stored results (reference results) obtained by querying the service providing system concerning an electronic ticket that is examined.

[1029] The information stored in the service data area 2401 will now be described in detail.

[1030] Fig. 25 is a detailed, specific diagram showing the relationships established for information stored in the service data area 2401.

[1031] The data management information 2405 consists of nine types of information: a last data update date 2500, a next data update date 2501, a terminal status 2502, a merchant information address 2503, a merchant public key certificate address 2504, a merchant preference address 2505, a ticket list address 2506, a transaction list address 2507 and an authorization report list address 2508.

[1032] The last data update date 2500 represents the date on which the service providing system 110 last updated the data in the RAM 2202 and on the hard disk 2203, and the next data update date 2501 represents the date on which the service providing system 110 will next update the data in the service data area 2401. The gate terminal 101 automatically initiates an update process when the time set according to the next data update date 2401 has been reached.

[1033] The time for the next data update date 2501 is set in the update time register 2301. When the next data update date 2501 is reached, the gate terminal 101 initiates the data updating process. During the data updating process, the service providing system 110 updates data stored in the RAM and on the hard disk. This process is performed daily at a time (e.g., late at night) at which communication traffic is not very heavy. The data updating process will be described in detail later.

[1034] The terminal status 2502 represents the status of the gate terminal. The merchant information address 2503, the merchant public key certificate address 2504, the merchant preference address 2505, the ticket list address 2506, the transaction list address 2507, and the authorization list address 2508 respectively represent the first addresses for the areas in which are stored the merchant information 2406, the merchant public key certificate 2407, the merchant preference information 2408, the ticket list 2409, the transaction list 2410, and the authorization list 2411.

[1035] List information for electronic tickets that are to be examined by the gate terminal 101 is stored in the ticket list 2409. An electronic ticket to be examined by the gate terminal 101 is set up either by the service providing system in the data updating process, or by the merchant downloading, from the service providing system, a program module (ticket examination module) for examining an electronic ticket (ticket examination setup). This setup method is determined in accordance with the contents of a contract entered into by the merchant and the service providing system.

[1036] Generally, when the usage form of the type of ticket to be examined at the gate terminal 101 must be frequently changed, for example, when, as at a stadium, the ticket to be examined is changed every day, depending on the event, or when the changing of the ticket to be examined depends on the individual gates (gate terminals), the merchant sets up the ticket to be examined. But when the type of ticket to be examined is changed less frequently and, for example, when as at a theme park a ticket to be examined is determined for each attraction, the service system providing system sets up the ticket to be examined.

[1037] In the ticket list 2409, for one electronic ticket type seven types of information are stored: a ticket name 2509, a ticket code 2510, a ticket issuer ID 2511, a validity term 2512, a gate private key 2513, a ticket public key 2514, and a ticket examination module address 2515. The ticket name 2509 is information that contains the name of an electronic ticket to be examined by the gate terminal 101; the ticket code 2510 is code information describing the type of the electronic ticket; and the validity term 2512 is the period the electronic ticket is valid for use. The gate private key 2513 and the ticket public key 2514 are encryption keys that respectively are paired with the gate public key 1912 and the ticket private key 1911 for the electronic ticket.

[1038] The ticket examination module address 2515 is an address on the hard disk 2203 whereat is stored the ticket examination module for the pertinent electronic ticket.

[1039] In the transaction list 2410, list information is stored for managing the history of the ticket examination process of the electronic ticket service. For one ticket examination process, four information items are stored in the transaction list 2410: a transaction number 2516, a service code 2517, a transaction time 2518, and a transaction information address 2519.

[1040] The transaction number 2516 is a number uniquely identifying the ticket examination process (from the view of the merchant); the service code 2517 is code information describing the type of mobile electronic commerce service that was provided for the user; and the transaction time 2518 is the time at which the ticket examination process was performed.

[1041] The transaction information address 2519 is an address at which is stored a ticket examination response 6703 that corresponds to the history information accumulated for the ticket examination process. In the transaction information address 2519 is stored a local address that points to an address on the hard disk 2203 or a remote address that points to indicates an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the transaction information address 2519, and when the merchant accesses the history information, the gate terminal 101 downloads the history information from the service providing system to the temporary area and displays it on the LCD.

[1042] The address stored at the transaction information address 2519 is determined by the service providing system. In the data updating process, the transaction times for the history information items are compared, and a local address is assigned for the history information having the latest transaction time. When there is adequate space on the hard disk 2203, all the transaction information addresses can be local addresses.

[1043] A list of authorization report addresses 2520, which are addresses at which the results of ticket references are stored, is stored in the authorization report list 2411 as list information for managing the results of the ticket reference process.

[1044] In the authorization report address 2520 is stored a local address that points to an address on the hard disk 2203 or to a remote address that points to an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the authorization report address 2520, and when the merchant accesses the authorization report, the gate terminal 101 downloads the authorization report from the service providing system to the temporary area, and displays it on the LCD.

[1045] The address stored at the authorization report address 2520 is determined by the service providing system. In the data updating process, the issue dates for the authorization reports are compared, and a local address is assigned for that information which has the latest issue date. When adequate space is available on the hard disk 2203, all the authorization report addresses can be local addresses.

[1046] The internal structure of the merchant terminal 102 will now be explained.

[1047] Fig. 26 is a block diagram illustrating the arrangement of the merchant terminal 102. The merchant terminal 102 comprises: a CPU (Central Processing Unit) 2600, which processes data that is to be transmitted and data that is received in accordance with a program stored in a ROM (Read Only Memory) 2601 and which controls the other components via a bus 2629; a RAM (Random Access Memory) 2602 and a hard disk 2603, whereat are stored data that are to be processed and data that have been processed by the CPU 2600; a EEPROM (Electric Erasable Programmable Read Only Memory) 2604, in which is stored the accounting machine ID of the merchant terminal 102, the terminal ID and the telephone number

as a telephone terminal, a merchant ID, a private key and a public key for the digital signature of a merchant, the service provider ID, a telephone number of a service providing system (the telephone number of the service providing system is accompanied by the digital signature of a service provider), and the public key of the service provider; an LCD controller 2605, which operates the LCD 502 under the control of the CPU 2600 and which displays on the LCD 502 an image set by the CPU 2600; a cryptographic processor 2606, which encrypts or decrypts data under the control of the CPU 2600; a data codec 2607, which encodes data to be transmitted and decodes data that is received under the control of the CPU 2600; an infrared communication module 501, which performs infrared communication with the mobile user terminal 100; a serial port 2609, which is connected to the infrared communication module 501; a serial-parallel converter 2608, which performs the bidirectional conversion of parallel data and serial data; a key operator 2611, which detects the manipulation of a mode switch 504 by a merchant, a hook switch 505, a function switch 506, a number key switch 507, an execution switch 508 or a power switch 509; an audio processor 2613, which drives a loudspeaker 2612 and the receiver of a telephone handset 503, and which amplifies an analog audio signal 2444 received at the microphone of the telephone handset 503 and supplies the resultant signal to an audio codec 2614; the audio codec 2414, which encodes an analog audio signal 2644 to provide digital audio data and decodes digital audio data to provide an analog audio signal 2643; a channel codec 2615, which multiplexes digital audio data and data-communication data in order to generate data to be transmitted, and which extracts digital audio data and data-communication data from multiplexed data that are received; a digital communication adaptor 2616, which is a communication adaptor employed with the digital communication telephone line 122; an RS-232C interface 2617, which is an interface circuit for the RS-232C cable 514 connected to the cash register 511; and a control logic unit 2610, which processes an interrupt signal received from the key operator 2613, the channel codec or the RS-232C interface 2617, and which serves as an interface when the CPU 2600 accesses the internal register of the key operator 2613, the audio processor 2613, the audio codec 2614 or the channel codec.

[1048] The cryptographic processor 2606 includes a secret key encryption and decryption function and a public key encryption and decryption function. The cryptographic processor 2606 employs a cryptography method determined by the CPU 2600 and the keys to encrypt or decrypt data selected by the CPU 2600. The CPU 2600 employs the encryption and decryption functions of the cryptographic processor 2606 to perform a digital signature process or a closing process for a message, and to decrypt a closed and encrypted message or to verify a digital signature accompanying a message. A detailed explanation will be given later for the digital signature process, the closing process, the decryption process and the digital signature verification process.

[1049] The data codec 2607 encodes data to be transmitted or decodes data that are received under the control of the CPU 1500. In this case, the encoding is a process for generating data to be transmitted that includes communication control information and error correction information, and the decoding is a process for performing error correction for the received data and for removing extra communication control information in order to obtain the data that a sender was to originally transmit. The data codec 2607 has a function for encoding or decoding data during data communication using a digital wireless telephone, and a function for encoding or decoding data during infrared communication. The data codec 2607 performs encoding or decoding as determined by the CPU for data that are selected by the CPU.

[1050] When, for example, a closed message accompanied by a digital signature is to be transmitted via digital telephone communication, the CPU 2600 employs the cryptographic processor 2606 to perform a digital signature process and a closing process for the message, employs the data codec 2607 to encode the obtained message to provide a data communication form for a digital telephone, and transmits the resultant message through the control logic unit 2610 to the channel codec 2615.

[1051] When a closed message accompanied by a digital signature is received via digital telephone communication, the CPU 2600 reads that message from the channel codec 2615 through the control logic unit 2610, employs the data codec 2607 to decode the received message, and permits the cryptographic processor 2606 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1052] Similarly, when a closed message accompanied by a digital signature is to be transmitted via infrared communication, the CPU 2600 employs the cryptographic processor 2606 to provide a digital signature for the message and to close the message, and employs the data codec 2607 to encode the obtained message to provide a data form suitable for infrared communication. Then, the resultant message is transmitted to the serial-parallel converter 2608.

[1053] When a closed message accompanied by a digital signature is received via infrared communication, the CPU 2600 reads that message from the serial-parallel converter 2608, employs the data codec 2607 to decode the received message, and permits the cryptographic processor 2606 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1054] When the merchant depresses either the mode switch 504, the hook switch 505, the function switch 506, the number key switch 507, the execution switch 508 or the power switch 509, the key operator 2611 asserts an interrupt signal 2639 requesting that the CPU 2600 perform a process corresponding to the switch that was manipulated. As is shown in Fig. 27A, the key operator 2611 includes a key control register (KEYCTL) 2710 for setting a valid/invalid state for each switch. The CPU 2600 accesses the key control register (KEYCTL) 2710 to determine whether a switch is effective or not.

[1055] The audio processor 2613 includes an audio control register (SCTL) 2709 for controlling the audio process, as is shown in Fig. 27A. The CPU 2600 accesses the audio control register (SCTL) 2709 to control the operation of the audio processor 2613. When, for example, a request for a digital telephone call is received, the CPU 2600 accesses the audio control register (SCTL) 2709 to output an arrival tone for a digital call. Therefore, the audio processor 2613 drives the loudspeaker 2612 to output an arrival tone for a digital call. It should be noted, however, that when a call request is from the service providing system 110, no arrival tone is output, and the CPU 2600 initiates a process for establishing a communication session with the service providing system.

[1056] The audio codec 2614 encodes an analog audio signal 2644 received from the audio processor 2613 to provide digital audio data, and decodes digital audio data read from the channel codec 2615 to provide an analog audio signal 2643. The analog audio signal 2643 is transmitted to the audio processor 2613, which amplifies the signal 2643 and drives the receiver of the telephone handset 2613 to release sounds from the receiver. The encoded digital audio data are transmitted to the channel codec 2615, which then changes the data into data that are suitable for transmission.

[1057] In addition, the audio codec 2614 includes an audio data encryption key register (CRYPT) 2711 in which is stored an encryption key for the secret key cryptography method that is employed for the encryption and decryption of audio data. When the audio data encryption key is set to the audio data encryption key register (CRYPT) 2711 by the CPU 2600, the audio codec 2614 encodes the analog audio signal 2644 to provide digital audio data while at the same time encrypting the digital audio data, or decodes the digital audio data to provide an analog audio signal 2643 while at the same time decrypting the digital audio data.

[1058] Two types of data to be transmitted are received by the channel codec 2615: one type is digital audio data received as a digital audio signal 2647 from the audio codec 2614, and the other type is data-communication data received from the CPU via the control logic unit 2610.

[1059] The channel codec 2615 adds, as header information, identification information for the digital audio data or the data-communication data to the respective data, and multiplexes the digital audio data and the data-communication data and transmits a resultant digital signal 2616 to the digital communication adaptor 2616.

[1060] In addition, upon receiving a digital signal 2648 from the digital communication adaptor 2616, the channel codec 2615 examines a terminal ID, identifies the digital audio data and the data-communication data using the header information, and transmits these data respectively as a digital audio signal 2647 and a digital signal 2651 to the audio codec 2612 and the control logic unit 2610. Further, upon receiving a digital call or data-communication data, the channel codec 2615 asserts an interrupt signal 2649, and upon receiving digital audio data, brings a control signal 2645 low. The interrupt signal 2649 is a signal requesting that the CPU 2600 perform the process in response to the arrival of a digital call and a process for data-communication data. The control signal 2645 is a low-active signal for requesting that the audio codec 2614 process the received digital audio data.

[1061] In order to perform these processes, as is shown in Fig. 27A, the channel codec 2615 includes: an ID register (ID) 2703, in which a terminal ID is stored; a channel codec control register (CHCTL) 2704, which controls the operation of the channel codec 2615; an audio transmission buffer 2705, in which are stored digital audio data received from the audio codec 2614; an audio reception buffer 2706, in which are stored digital audio data extracted from received data; a data transmission buffer 2707, in which are stored

data-communication data received from the CPU 2600 via the control logic unit 2610; and a data reception buffer 2708, in which are stored data-communication data extracted from received data.

[1062] A control signal 2646 is a control signal with which the audio codec 2614 directs the channel codec 2514 to write data to the data transmission buffer 2705 and to read data from the data reception buffer 2706. The audio codec 2614 sets the control signal 2646 low to write the digital audio data to the data transmission buffer 2705, and sets the control signal 2646 high to read the digital audio data from the data reception buffer 2706.

[1063] A control signal 2650 is a control signal with which the CPU 2600 directs the channel codec 2615 via the control logic unit 2610 to write data to the data transmission buffer 2707 and to read data from the data reception buffer 2708. When the control signal 2650 goes low, the data-communication data are written to the data transmission buffer 2707, and when the control signal 2650 goes high, the data-communication data are read from the data reception buffer 2708.

[1064] The digital communication adaptor 2616 encodes a digital signal 2648 to obtain data having a format suitable for digital telephone communication, and outputs the resultant signal to a digital telephone communication line 122. The digital communication adaptor 2616 further decodes a signal received along the digital telephone communication line 122, and supplies an obtained digital signal 2648 to the channel codec 2615.

[1065] The RS-232C interface 2617 is an interface circuit for connecting the RS-232C cable 514. The merchant terminal 102 communicates with the cash register 511 via the RS-232C interface 2617. The RS-232C interface 2617 receives data from the cash register 511 and asserts an interrupt signal 2652. The interrupt signal 2652 is a signal requesting that the CPU 2600 exchange data with the cash register 511 via the RS-232C interface 2617.

[1066] The control logic unit 2610 internally includes three registers, as is shown in Fig. 27A: a clock counter (CLOCKC) 2700, an update time register (UPTIME) 2701, and an interrupt register (INT) 2702.

[1067] The clock counter 2700 measures the current time; the update time register 2701 is used to store the time at which the merchant terminal 102 updates data in the RAM 2602 and on the hard disk 2603 through communication conducted with the service providing system (data updating process); and the interrupt register 2702 is used to indicate the reason an interrupt for the CPU 2600 is generated.

[1068] When the count in the clock counter 2700 matches the count in the update time register 2701, and when one of the interrupt signals 2639, 2649 and 2652 is asserted, the control logic unit 2610 writes the reason the interrupt was generated in the interrupt register (INT) 2702, and asserts an interrupt signal 2618 requesting that the CPU 2600 perform the interrupt process. For the interrupt process, the CPU 2600 reads from the interrupt register the reason the interrupt was generated, and performs a corresponding process.

[1069] The individual bit fields in the interrupt register (INT) are defined as is shown in Fig. 27B.

[1070] Bit 31 represents the state of the power switch. When the bit value is 0, it represents the power-OFF state, and when the bit value is 1, it represents the power-ON state.

[1071] Bit 30 represents the digital telephone communication state. When the bit value is 0, it represents the state during which no digital telephone communication is being performed, and when the bit value is 1, it represents the state during which digital telephone communication is being performed.

[1072] Bit 28 represents the generation of a call arrival interrupt. When the bit value is 1, it signals the arrival of a digital call. In this bit field, a 1 is set when a digital telephone call is received and the interrupt signal 2649 is asserted.

[1073] Bit 27 represents the generation of a data reception interrupt. When the bit value is 1, it signals the reception of data. In this bit field, a 1 is set when the data-communication data are received and the interrupt signal 2649 is asserted during the conduct of digital telephone communication.

[1074] Bit 26 represents the generation of an update interrupt requesting the performance of a data updating process. When the bit value is 1, it signals the generation of the update interrupt. In this bit field, a 1 is set when the count in the clock counter matches the count in the update time register.

[1075] Bit 25 represents the generation of an external IF interrupt requesting that data communication with the cash register 311 be initiated. When the bit value is 1, it signals the generation of the external IF interrupt. In this bit field, a 1 is set when the interrupt signal 2652 received from the RS-232C interface 2617 is asserted.

[1076] Bit 24 represents the generation of a key interrupt by the manipulation of a switch. When the bit value is 1, it represents the generation of the key interrupt.

[1077] Bits 0 to 9 correspond to switches 0 to 9 of the number key switches. Bits 10 and 11 correspond to number key switches "*" and "#," and bits 12 to 15 correspond to function switches F1 to F4. Bits 16 to 18 respectively correspond to the power switch, the execution switch, the mode switch and the speech switch, and bit 20 corresponds to the hook switch. When a bit value is 1, it indicates that a switch corresponding to the bit has been depressed.

[1078] Data stored in the RAM 2602 will now be described.

[1079] Fig. 28 is a specific diagram of a RAM map for data stored in the RAM 2602.

[1080] The RAM 2602 is constituted by five areas: a fundamental program object area 2800, a service data area 2801, a merchant area 2802, a work area 2803 and a temporary area 2804. In the fundamental program object area 2800 are stored an upgraded module of a program stored in the ROM 2601, a patch program and an additional program. The merchant area 2802 is an area that a merchant can freely use, the work area 2803 is a work area that the CPU 100 employs when executing a program, and the temporary area 2804 is an area in which information received by the merchant terminal is stored temporarily.

[1081] The service data area 2801 is an area in which are stored contract information for the electronic commerce service, available credit card information, available payment card information and history information, and the data in this area are managed by the service providing system. The service data area 2801 is constituted by nine sub-areas: a data management information area 2805, a merchant information area 2806, a merchant public key certificate area 2807, a merchant preference area 2808, a telephony information area 2809, an available credit card list area 2810, an available payment card list 2811, a transaction list area 2812, and an authorization report list 2813.

[1082] The data management information area 2805 is an area in which is stored management information for data stored in the service data area 2801; the merchant information area 2806 is an area in which are stored the name of a merchant and information for the contents of a contract with a service provider; the merchant public key certificate area 2807 is an area in which a public key certificate for a merchant is stored; the merchant preference area 2808 is an area in which preference information for a merchant is stored that concerns the mobile electronic commerce service; the telephony information area 2809 is an area in which information concerning a digital telephone is stored; the available credit card list area 2810 is an area in which is stored list information for the credit cards the merchant can handle; the available payment card list area 2811 is an area in which is stored list information for the payment cards the merchant can handle; the transaction list area 2812 is an area in which is stored sales history information for the mobile electronic commerce service; and the authorization report list area 2813 is an area in which are stored the results (micro-check reference results) that are obtained by the service providing system when it examines the micro-check that is handled.

[1083] The information stored in the service data area 2801 will now be described in detail.

[1084] Fig. 29 is a detailed, specific diagram showing the relationships established for information stored in the service data area 2801.

[1085] The data management information 2805 consists of eleven types of information: a last data update date 2900, a next data update date 2901, a terminal status 2902, a merchant information address 2903, a merchant public key certificate address 2904, a merchant preference address 2905, a telephony information address 2906, an available credit card list address 2907, an available payment card list address 2908, a transaction list address 2909, and an authorization report list address 2910.

[1086] The last data update date 2900 represents the date on which the service providing system 110 last updated the data in the RAM 2602 and on the hard disk 2603, and the next data update date 2901

represents the date on which the service providing system 110 will next update the data in the service data area 2801. The merchant terminal 102 automatically initiates an update process when the is reached that is set according to the next data update date 2901.

[1087] The time for the next data update date 2901 is set in the update time register 2701. When the next data update date 2901 is reached, the merchant terminal 102 initiates the data updating process. During the data updating process, the service providing system 110 updates data stored in the RAM and on the hard disk. This process is performed daily during a period (e.g., late at night) in which communication traffic is not very heavy. The data updating process will be described in detail later.

[1088] The terminal status 2902 represents the status of the merchant terminal 102. The merchant information address 2903, the merchant public key certificate address 2904, the merchant preference address 2905, the telephony information address 2906, the available credit card list address 2907, the available payment card list address 2908, the transaction list address 2909 and the authorization report list address 2910 respectively represent the first addresses for the areas in which are stored the merchant information 2806, the merchant's public key certificate 2807, the merchant preference information 2808, the telephony information 2809, the available credit card list 2910, the available payment card list 2811, the transaction list 2812 and the authorization report list 2813.

[1089] The telephony information area 2809 includes three types of information: a last called number 2911, an address book address 2912 and a shortcut file address 2913. The last called number 2911 represents a telephone number for a prior call placed by the merchant, and is employed for the redialing of a digital telephone. The address book address 2912 and the shortcut file address 2913 respectively represent addresses on the hard disk 2603 at which address book information and a shortcut file are stored.

[1090] The available credit card list 2810 includes list information for those credit cards that can be handled by a merchant. In the available credit card list 2810, three types of information are entered for each credit card: a credit card name 2914, a service code list address 2915, and a credit card clearing program address 2916. The credit card name 2914 represents the name of a credit card that the merchant can handle, and the service code list address 2915 is an address on the hard disk 2603 at which is stored a service code list that shows the types of services that can be provided by the merchant when the electronic credit card is used. The service code list is a list of payment service codes and optional payment codes that the merchant can handle.

[1091] The credit card clearing program address 2916 is an address on the hard disk 2603 at which is stored a credit card clearing program for the pertinent electronic credit card.

[1092] The available payment card list 2811 includes list information for payment cards that can be handled by a merchant.

[1093] In the available payment card list 2811, for each payment card, seven types of information are entered: a card name 2917, a card code 2918, a payment card issuer ID 2919, a validity term 2920, an accounting machine private key 2921, a card public key 2922, and a payment card accounting module address 2923. The card name 2917 represents the name of a payment card that the merchant can handle; the card code 2918 is code information that represents the type of electronic payment card; the payment card issuer ID 2919 is ID information for a payment card issuer; and the validity term 2920 is the period during which the electronic payment card is valid. The accounting machine private key 2921 and the card public key 2922 are encryption keys that are respectively paired with the accounting machine public key 2012 and the card private key 2011 for the electronic payment card.

[1094] The payment card accounting module address 2923 is an address on the hard disk 2603 at which is stored a program module (a payment card accounting module) for clearing the electronic payment card.

[1095] In accordance with the contract entered into by the merchant and the service providing system, the service providing system sets up or updates the contents of the available payment card list 2811 in the data updating process.

[1096] In the transaction list 2812, list information is stored to manage the history information for sales through the mobile electronic commerce service. For the sales effected through one mobile electronic commerce service, in the transaction list 2812 are stored four information items: a transaction number 2924, a service code 2925, a transaction time 2926, and a transaction information address 2927.

[1097] The transaction number 2924 is a number uniquely identifying a transaction performed with a user (from the view of the merchant); the service code 2925 is code information identifying the type of mobile electronic commerce service that was provided for the user; and the transaction time 2926 is time information for the time at which a product was sold or the service was provided via the mobile electronic service.

[1098] The transaction information address 2927 is an address at which is stored a micro-check that describes the contents of the sale and a receipt. In the transaction information address 2927 is stored a local address that points to an address on the hard disk 2603 or a remote address that indicates an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the transaction information address 2927, and when the merchant accesses the sales history information, the merchant terminal 102 downloads the history information from the service providing system to the temporary area, and displays it on the LCD.

[1099] The address stored at the transaction information address 2927 is determined by the service providing system. In the data updating process, the transaction times for the sales history information items are compared, and a local address is assigned for the sales information having the latest transaction time. When there is adequate space on the hard disk 2603, all the transaction information addresses can be local addresses.

[1100] A list of authorization report addresses 2928, which are addresses at which the results of the reference of the micro-check are stored, is stored in the authorization report list area 2813 as list information for managing the results of the micro-check reference process.

[1101] In the authorization report address 2928 is stored a local address that indicates an address on the hard disk 2603 or a remote address that indicates an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the authorization report address 2928, and when the merchant accesses the authorization report, the merchant terminal 102 downloads the authorization report from the service providing system to the temporary area, and displays it on the LCD.

[1102] The address stored at the authorization report address 2928 is determined by the service providing system. In the data updating process, the issuing dates for the authorization reports are compared, and a local address is assigned for the information having the latest issuing date. When there is adequate space on the hard disk 2603, all the authorization report addresses can be local addresses.

[1103] The internal structure of the merchant terminal 103 will now be described.

[1104] Fig. 30 is a block diagram illustrating the arrangement of the merchant terminal 103. This terminal 103 comprises: a CPU (Central Processing Unit) 3000, which employs a program stored in a ROM (Read Only Memory) 3001 to process data for transmission and for reception, and to control the other components via a bus 3029; a RAM (Random Access Memory) 3002, in which are stored data that are processed and are to be processed by the CPU 3000; a EEPROM (Electric Erasable Programmable Read Only Memory) 3003, in which is stored an accounting machine ID for the merchant terminal 103, a terminal ID and a telephone number for the merchant terminal 103 when used as a wireless telephone terminal, a merchant ID, a private key and a public key for a merchant digital signature, a service provider ID, and the telephone number and the public key of the service providing system 110 (the digital signature of the service provider accompanies the telephone number of the service providing system); an LCD controller 3004, which operates the LCD 603 under the control of the CPU 3000, and which displays on the LCD an image that is selected by the CPU 3000; a cryptographic processor 3005, which encrypts and decrypts data under the control of the CPU 3000; a data codec 3006, which encodes data to be transmitted and decodes received data under the control of the CPU 3000; a memory card 3059 on which product information is recorded and a card slot 614 for the memory card; an infrared communication module 3007, which transmits and receives infrared rays during infrared communication; a bar code reader 610 for reading the bar code of a product; a key operator 3009, which detects the manipulation by the user of a mode switch 604, a speech switch 605, an end switch 606, a function switch 607, a number key switch 608, a power switch 611 and an execution switch 612; an audio processor 3011, which drives a loudspeaker 3010, a receiver 602 or a headphone set that is connected to a headphone jack 612, and which amplifies an analog audio signal that is input through a microphone 609 or the headphone head; an audio codec 3012, which encodes an analog audio signal 3042 to provide digital audio data, and which decodes digital audio data to provide an analog audio signal 3043; a channel codec 3013, which generates data to be transmitted along a radio channel, and which

extracts, from received data, data that is addressed to the merchant terminal 103; a modulator 3014, which modulates a serial digital signal 3047 input by the channel codec 3013 to obtain an analog transmission signal 3049 that employs as a baseband an electric signal 3052 that is transmitted by a PLL 3016; a demodulator 3015, which demodulates an analog signal 3050 that is received while employing as a baseband an electric signal 3053 that is supplied by the PLL 3016, and which transmits a serial digital signal 3048 to the channel codec 3013; an RF unit 3017, which changes the analog transmission signal 3049 received from the modulator 3014 into a radio wave and outputs it through an antenna 601, and which, upon receiving a radio wave through the antenna 601, transmits an analog reception signal 3050 to the demodulator 3015; a battery capacity detector 3018, which detects the capacity of the battery of the merchant terminal 103; and a control logic unit 3008, which activates the channel codec 3013, the PLL 3016 and the RF unit 3017, and which processes interrupt signals that are transmitted by the key operator 3009, the channel codec 3013 and the battery capacity detector 3018, and which serves as an interface when the CPU 3000 accesses the internal registers of the key operator 3009, the audio processor 3011, the audio codec 3012 and the channel codec.

[1105] On the memory card 3059, the name of a product, a product code, a bar code and a price are recorded as product information. Based on the bar code of the product that is read by the bar code reader 610, the CPU 3000 accesses the product information on the memory card 3059 to calculate the amount of a charge.

[1106] The cryptographic processor 3005 includes a secret key encryption and decryption function and a public key encryption and decryption function. The cryptographic processor 3005 employs a cryptography method determined by the CPU 3000 and the keys to encrypt or decrypt data selected by the CPU 3000. The encryption and decryption functions of the cryptographic processor 3005 are employed to perform a digital signature process or a closing process for a message, and to decrypt a closed and encrypted message or to verify a digital signature accompanying a message. A detailed explanation will be given later for the digital signature process, the closing process, the decryption process and the digital signature verification process.

[1107] The data codec 3006 encodes data to be transmitted or decodes data that is received, under the control of the CPU 3000. In this case, the encoding is a process for generating data to be transmitted that includes communication control information and error correction information, and the decoding is a process for performing error corrections for the received data and for removing extra communication control information in order to obtain the data that a sender was to originally transmit. The data codec 3006 has a function for encoding or decoding data during data communication conducted using a digital wireless telephone, and a function for encoding or decoding data during infrared communication. The data codec 3006 performs the encoding or decoding, as determined by the CPU 3000, of data that are selected by the CPU 3000.

[1108] When, for example, a closed message accompanied by a digital signature is to be transmitted via digital wireless telephone communication, the CPU 3000 employs the cryptographic processor 3005 to perform a digital signature process and a closing process for a message, employs the data codec 3006 to encode the obtained message to provide a data communication form for a digital wireless telephone, and transmits the resultant message through the control logic unit 3008 to the channel codec 3013.

[1109] When a closed message accompanied by a digital signature is received via digital wireless telephone communication, the CPU 3000 reads that message from the channel codec 3013 through the control logic unit 3008, employs the data codec 3006 to decode the received message, and permits the cryptographic processor 3005 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1110] Similarly, when a closed message accompanied by a digital signature is to be transmitted via infrared communication, the CPU 3000 employs the cryptographic processor 3005 to provide a digital signature for the message and to close the message, and employs the data codec 3006 to encode the obtained message to provide a data form that is suitable for infrared communication. Then, the resultant message is transmitted to the infrared communication module 3007.

[1111] When a closed message accompanied by a digital signature is received via infrared communication, the CPU 3000 reads that message from the infrared communication module 3007, employs the data codec 3006 to decode the received message, and permits the cryptographic processor 3005 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1112] When the merchant depresses either the mode switch 604, the speech switch 605, the end switch 606, the function switch 607, the number key switch 608, the power switch 611 or the execution switch 612, the key operator 3009 detects the switch manipulation by the user and asserts an interrupt signal 3038 requesting the performance of a process corresponding to the switch that was manipulated. As is shown in Fig. 31A, the key operator 3009 includes a key control register (KEYCTL) 3112 for setting the valid/invalid state of each switch. The CPU 3000 accesses the key control register (KEYCTL) 3112 to set the valid/invalid state of each switch.

[1113] The audio processor 3011 includes an audio control register (SCTL) 3111 for controlling the audio process, as is shown in Fig. 31A. The CPU 3000 accesses the audio control register (SCTL) 3111 to control the audio processor 3011. When, for example, a call request is received over a digital wireless telephone, the CPU 3000 accesses the audio control register (SCTL) 3111 to output a call tone for a digital wireless telephone. As a result, the audio processor 3011 drives the loudspeaker 3010 to release the call tone for a digital wireless telephone. It should be noted that when a call request is from the service providing system 110, no call arrival tone is output, and the CPU 3000 initiates a process for establishing a communication session with the service providing system.

[1114] The audio codec 3012 encodes an analog audio signal 3042 received from the audio processor 3011 to provide digital audio data, and decodes digital audio data received from the channel codec 3013 to provide an analog audio signal 3043. The analog audio signal 3043 is transmitted to the audio processor 3011, which amplifies the signal 3043 and drives the receiver 602 to produce sounds. The encoded digital audio data are transmitted as a digital audio signal 3046 to the channel codec 3013, which converts the data into data that can be transmitted across the radio channel.

[1115] In addition, the audio codec 3012 includes an audio data encryption key register (CRYPT) 3113 in which is stored an encryption key for the secret key cryptography method that is employed for the encryption and decryption of audio data. When the audio data encryption key is set to the audio data encryption key register (CRYPT) 3113 by the CPU 3000, the audio codec 3012 encodes the analog audio signal 3042 to provide digital audio data while at the same time encrypting the digital audio data, or decodes the digital audio data to provide an analog audio signal 3043 while at the same time decrypting the digital audio data.

[1116] Two types of data to be transmitted are received by the channel codec 3013: one type is digital audio data originating at the audio codec 3012 as a digital audio signal 3046, and the other type is data-communication data originating at the CPU 3000 that pass through the control logic unit 3008 as a digital signal 3056.

[1117] The channel codec 3013 adds identification data, as header information, to digital audio data and data-communication data, then converts the data into a serial digital signal 3047 having a data format that is suitable for a digital wireless telephone, and transmits the signal 3047 to the modulator 3014.

[1118] In addition, upon receiving a serial digital signal 3048 from the demodulator 3015, the channel codec 3013 examines a terminal ID and extracts only such data as is addressed to the channel codec 3013, removes the communication control information for the digital wireless telephone, identifies the digital audio data and the data-communication data in the header information, and transmits these data as a digital audio signal 3046 and a digital signal 3056 to the audio codec 3012 and the control logic unit 3008 respectively.

[1119] Further, upon receiving a digital wireless call or data-communication data, the channel codec 3013 asserts an interrupt signal 3054, and upon receiving digital audio data, brings the control signal 3044 low. The interrupt signal 3054 is a signal requesting that the CPU 3000 perform the process for a received digital wireless phone communication and a process for data-communication data. The control signal 3044 is a low-active signal for requesting that the audio codec 3012 process the received digital audio data.

[1120] In order to perform these processes, as is shown in Fig. 31A, the channel codec 3013 includes: an ID register (ID) 3105, in which is stored a terminal ID; a channel codec control register (CHCTL) 3106, which controls the operation of the channel codec 3013; an audio transmission buffer 3107, in which are stored digital audio data received from the audio codec 3012; an audio reception buffer 3108, in which are stored digital audio data extracted from received data; a data transmission buffer 3109, in which are stored data-communication data received from the control logic unit 3008; and a data reception buffer 3110, in

which are stored data-communication data extracted from received data.

[1121] A control signal 3045 is a control signal with which the audio codec 3012 directs the channel codec 3013 to write data to the data transmission buffer 3107 and to read data from the data reception buffer 3108. When the control signal 3045 goes low, the digital audio data are written to the data transmission buffer 3107, and when the control signal 3045 goes high, the digital audio data are read from the data reception buffer 3109.

[1122] A control signal 3055 is a control signal with which the CPU 3000 directs the channel codec 3013 via the control logic unit 3008 to write data to the data transmission buffer 3109 and to read data from the data reception buffer 3110. When the control signal 3055 goes low, the data-communication data are written to the data transmission buffer 3109, and when the control signal 3055 goes high, the data-communication data are read from the data reception buffer 3110.

[1123] The modulator 3014 modulates a serial digital signal 3047 received from the channel codec 3013 to provide an analog transmission signal 3049, which is employed as a baseband for an electric signal 3052 that is supplied by the PLL 3016, and transmits the signal 3049 to the RF unit 3017. The analog transmission signal 3049 received by the RF unit 3017 is output as a radio wave through the antenna 601.

[1124] When a radio wave is received at the antenna 601, an analog reception signal 3050 is transmitted by the RF unit 3017 to the demodulator 3015. The demodulator 3015 demodulates the analog signal 3050, while employing as its baseband an electric signal 3053 that is supplied by the PLL 3016, and transmits an obtained serial digital signal 3048 to the channel codec 3013.

[1125] The battery capacity detector 3018, for detecting the capacity of a battery, asserts an interrupt signal 3057 when the remaining capacity of the battery of the merchant terminal 103 is equal to or less than an amount Q (Q > 0) that is set by the CPU 3000. The interrupt signal 3057 is a signal for requesting that the CPU 3000 perform a data backup process for the RAM 3002. The amount Q is large enough to enable the merchant terminal 103 to communicate with the service providing system 110 in order to back up data in the RAM 3002 for the service providing system 110 (data backup process).

[1126] The control logic unit 3008 includes six internal registers, as is shown in Fig. 31A: a frame counter (FRAMEC) 3100, a start frame register (FRAME) 3101, a clock counter (CLOCKC) 3102, an update time register (UPTIME) 3103, an interrupt register (INT) 3104, and a key display register (KEY) 3114.

[1127] The frame counter 3100 is employed to count the number of frames for the digital wireless telephone; the start frame register 3101 is employed to store the frame number of the frame that is to be activated next; the clock counter 3102 is employed to measure the current time; the update time register 3103 is employed to store the time at which the merchant terminal 103 will communicate with the service providing system 110 to update data in the RAM 3002 (data updating process); the interrupt register 3104 is employed to indicate the type of interrupt that is generated for the CPU 3000; and the key display register (KEY) 3114 is employed to indicate the reason the interrupt is generated by key manipulation.

[1128] Generally, to receive a call, the digital wireless telephone intermittently acquires control data for a control channel and compares it with the terminal ID. The merchant terminal 103 employs the frame counter 3100 and the start frame register 3101 to intermittently acquire control data. First, the frame number of the frame to be activated next is stored in advance in the start frame register 3101, and when the count held by the frame counter 3100 equals the count held by the start frame register 3101, to acquire control data the control logic unit 3008 activates the channel codec 3013, the PLL 3016 and the RF unit 3017 via an address data signal line 3058.

[1129] When the count held by the clock counter 3102 matches the count held by the update time register 3103, or when one of the interrupt signals 3058, 3054 and 3057 is asserted, the control logic unit 3008 writes the type of and the reason for the interrupt in the interrupt register (INT) 3104 and in the key display register (KEY) 3114, and asserts an interrupt signal 3019 requesting that the CPU 3000 perform an interrupt process. For the interrupt processing, the CPU 3000 reads the type of and the reason for the interrupt that are stored in the interrupt register (INT) 3104 and the key register (KEY) 3114, and then performs a corresponding process.

[1130] The individual bit fields of the interrupt register (INT) 3104 are defined as is shown in Fig. 31B.

[1131] Bit 31 represents the state of the power switch 611. When the bit value is 0, it indicates the state is the power-OFF state, and when the bit value is 1, it indicates the state is the power-ON state.

[1132] Bit 30 represents the digital wireless telephone communication state. When the bit value is 0, it indicates the state is one where no digital wireless telephone communication is being performed, and when the bit value is 1, it indicates the state is one where digital wireless telephone communication is in process.

[1133] Bit 29 represents the generation of a frame interrupt requesting the intermittent acquisition of control data. When the bit value is 1, it indicates a condition that exists when a frame interruption has occurred. In this bit field, a 1 is set when the amount held by the frame counter 3100 equals the amount held by the start frame register 3101.

[1134] Bit 28 represents the generation of a call arrival interrupt. When the bit value is 1, it indicates that a digital wireless call has arrived. In this bit field, a 1 is set when the terminal ID is matched and the interrupt signal 3054 is asserted during the intermittent acquisition of control data for the digital wireless phone.

[1135] Bit 27 represents the generation of a data reception interrupt. When the bit value is 1, it indicates that data are being received. In this bit field, a 1 is set when the data-communication data are received and the interrupt signal 3054 is asserted during the course of a digital wireless telephone communication session.

[1136] Bit 26 represents the generation of an update interrupt requesting the performance of a data updating process. When the bit value is 1, it indicates the generation of the update interrupt. In this bit field, a 1 is set when the count held by the clock counter 3102 matches the count held by the update time register 3103.

[1137] Bit 25 represents the generation of a battery interrupt requesting a backup process. When the bit value is 1, it represents the generation of the battery interrupt. In this bit field, a 1 is set when the interrupt signal 3057 that is received from the battery capacity detector 3018 is asserted.

[1138] Bit 24 represents the generation of a key interrupt by the manipulation of the switch. When the bit value is 1, it represents the generation of the key interrupt.

[1139] The individual bit fields in the key display register (KEY) 3114 are defined as is shown in Fig. 31C.

[1140] Bits 31 to 25 correspond to switches "=," "+," "-," "x," " DIVIDED ," "." and total" for the number key switch 608. Bits 20 to 16 correspond to the end switch 606, the speech switch 605, the mode switch 604, the execution switch 612 and the power switch 611. Bits 15 to 12 correspond to switches "F4" to "F1" for function switch 307. Bits 11 and 10 respectively correspond to switches "#" and "*" for the number key switches. Bits 9 to 0 correspond to switches 9 to 0 for the number key switches 608. When the value of a bit is 1, it indicates that a switch corresponding to that bit has been depressed.

[1141] Data stored in the RAM 3002 will now be described.

[1142] Fig. 32 is a specific diagram of a RAM map for data stored in the RAM 3002.

[1143] The RAM 3002 is constituted by five areas: a fundamental program object area 3200, a service data area 3201, a merchant area 3202, a work area 3203 and a temporary area 3204. In the fundamental program object area 3200 are stored an upgraded module of a program stored in the ROM 3001, a patch program and an additional program. The merchant area 3202 is an area that a merchant can freely use, the work area 3203 is a work area that the CPU 100 employs when executing a program, and the temporary area 3204 is an area in which information received by the merchant terminal is stored temporarily.

[1144] The service data area 3201 is an area in which are stored contract information for the electronic commerce service, available credit card information, available payment card information and history information, and the data in this area are managed by the service providing system. The service data area 3201 is constituted by ten sub-areas: a data management information area 3205, a merchant information area 3206, a merchant public key certificate area 3207, a merchant preference area 3208, a telephony information area 3209, an available credit card list area 3210, an available payment card list 3211, a transaction list area 3212, an authorization report list 3213, and an object data area 3214.

[1145] The data management information area 3205 is an area in which is stored management information for data stored in the service data area 3201; the merchant information area 3206 is an area in which are stored the name of a merchant and information for the contents of a contract with a service provider; the merchant public key certificate area 3207 is an area in which a public key certificate for a merchant is stored; the merchant preference area 3208 is an area in which preference information for a merchant is stored that concerns the mobile electronic commerce service; the telephony information area 3209 is an area in which information concerning a digital wireless telephone is stored; the available credit card list area 3210 is an area in which is stored list information for those credit cards the merchant can handle; the available payment card list area 3211 is an area in which is stored list information for those payment cards the merchant can handle; the transaction list area 3212 is an area in which is stored sales history information for the mobile electronic commerce service; the authorization report list area 3213 is an area in which are stored the results (micro-check reference results) that are obtained from the service providing system by examining the micro-check that is handled; and the object data area 3114 is an area in which are stored object data for the information managed in the other nine areas.

[1146] The information stored in the service data area 3201 will now be described in detail.

[1147] Fig. 33 is a detailed, specific diagram showing the relationships established for information stored in the service data area 3201.

[1148] The data management information 3205 consists of eleven types of information: a last data update date 3300, a next data update date 3301, a terminal status 3302, a merchant information address 3303, a merchant public key certificate address 3304, a merchant preference address 3305, a telephony information address 3306, an available credit card list address 3307, an available payment card list address 3308, a transaction list address 3309, and an authorization report list address 3310.

[1149] The last data update date 3300 represents the date on which the service providing system 110 last updated the data in the RAM 3002, and the next data update date 3301 represents the date on which the service providing system 110 will next update the data in the service data area 3201. The merchant terminal 103 automatically initiates an update process when the time set according to the next data update date 3301 is reached.

[1150] The time of the next data update date 3301 is set in the update time register 3103. When the next data update date 3301 is reached, the merchant terminal 103 initiates the data updating process. During the data updating process, the service providing system 110 updates data stored in the RAM. This process is performed daily during a period (e.g., late at night) in which communication traffic is not very heavy. The data updating process will be described in detail later.

*[1151] The terminal status 3302 represents the status of the merchant terminal 103. The merchant information address 3303, the merchant public key certificate address 3304, the merchant preference address 3305, the telephony information address 3306, the available credit card list address 3307, the available payment card list address 3308, the transaction list address 3309 and the authorization report list address 3310 respectively represent the first addresses for the areas in which are stored the merchant information 3206, the merchant public key certificate 3207, the merchant preference information 3208, the telephony information 3209, the available credit card list 3210, the available payment card list 3211, the transaction list 3212 and the authorization report list 3213.

[1152] The telephony information area 3209 includes three types of information: a last called number 3311, an address book address 3312 and a shortcut file address 3313. The last called number 3311 represents a telephone number for a prior call placed by the merchant, and is employed for the redialing of a digital wireless telephone. The address book address 3312 and the shortcut file address 3313 respectively represent addresses in the object data area 3214 at which address book information and a shortcut file are stored.

[1153] The available credit card list 3210 includes list information for credit cards that can be handled by a merchant. In the available credit card list 3210, three types of information are entered for each credit card: a credit card name 3314, a service code list address 3315 and a credit card clearing program address 3316. The credit card name 3314 represents the name of a credit card that the merchant can handle, and the service code list address 3315 is an address in the object data area 3214 at which is stored a service code list that shows the types of services that can be provided by the merchant when the electronic credit card is

used. The service code list is a list of payment service codes and optional payment codes that the merchant can handle. The credit card clearing program address 3316 is an address in the object data area 3214 at which is stored a credit card clearing program for the pertinent electronic credit card.

[1154] The available payment card list 3211 includes list information for payment cards that can be handled by a merchant.

[1155] In the available payment card list 3211, for each payment card, seven types of information are entered: a card name 3317, a card code 3318, a payment card issuer ID 3319, a validity term 3320, an accounting machine private key 3321, a card public key 3322, and a payment card accounting module address 3323. The card name 3317 represents the name of a payment card that the merchant can handle; the card code 3318 is code information that represents the type of electronic payment card; the payment card issuer ID 3319 is ID information for a payment card issuer; and the validity term 3320 is the period during which the electronic payment card is valid. The accounting machine private key 3321 and the card public key 3322 are encryption keys that are respectively paired with the accounting machine public key 2012 and the card private key 2011 for the electronic payment card.

[1156] The payment card accounting module address 3323 is an address in the object data area 3214 in which is stored a program module (a payment card accounting module) for clearing the electronic payment card.

[1157] In accordance with the contract entered into by the merchant and the service providing system, the service providing system sets up or updates the contents of the available payment card list 3211 in the data updating process.

[1158] In the transaction list 3212, list information is stored to manage the history information for sales through the mobile electronic commerce service. For the sales effected through one mobile electronic commerce service, in the transaction list 3212 are stored four information items: a transaction number 3324, a service code 3325, a transaction time 3326, and a transaction information address 3327.

[1159] The transaction number 3324 is a number uniquely identifying a transaction performed with a user (from the view of the merchant); the service code 3325 is code information identifying the type of mobile electronic commerce service that was provided for the user; and the transaction time 3326 is time information for the time at which a product was sold or the service was provided via the mobile electronic service.

[1160] The transaction information address 3327 is an address at which is stored a micro-check that describes the contents of the sale and a receipt. In the transaction information address 3327 is stored a local address that points to an address in the object data area 3214 or a remote address that indicates an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the transaction information address 3327, and when the merchant accesses the sales history information, the merchant terminal 103 downloads the history information from the service providing system to the temporary area, and displays it on the LCD.

[1161] The address stored at the transaction information address 3327 is determined by the service providing system. In the data updating process, the transaction times for the sales history information items are compared, and a local address is assigned for the sales information having the latest transaction time. When there is adequate space on the ROM 3302, all the transaction information addresses can be local addresses.

[1162] A list of authorization report addresses 3328, which are addresses at which the results of the reference of the micro-check are stored, is stored in the authorization report list area 3213 as list information for managing the results of the micro-check reference process.

[1163] In the authorization report address 3228 is stored a local address that indicates an address in the object data area 3214 or a remote address that indicates an address in the merchant information server 903 of the service providing system 110. When the remote address is stored at the authorization report address 3328, and when the merchant accesses the authorization report, the merchant terminal 103 downloads the authorization report from the service providing system to the temporary area, and displays it on the LCD.

[1164] The address stored at the authorization report address 3328 is determined by the service providing system. In the data updating process, the issuing dates for the authorization reports are compared, and a local address is assigned for the information having the latest issuing date. When there is adequate space in the RAM 3002, all the authorization report addresses can be local addresses.

[1165] The internal structure of the automatic vending machine 104 will now be described.

[1166] Fig. 34 is a block diagram illustrating the arrangement of the automatic vending machine 104. The automatic vending machine 104 can be internally divided into two sections: an accounting machine 3455, and a sales mechanism 3456. The accounting machine 3455 is a unit for performing a payment card settlement process with the mobile user terminal 100, and the sales mechanism 3456 is a unit for performing another process, specifically, the calculation and display of the price of a product selected by a user, the discharge of the product to a discharge port 703, and the management of the products in stock.

[1167] In Fig. 34, the accounting machine 3455 comprises: a CPU (Central Processing Unit) 3400, which employs a program stored in a ROM (Read Only Memory) 3401 to process data for transmission and for reception and to control the other components via a bus 3445; a RAM (Random Access Memory) 3402, in which are stored data that are being processed and are to be processed by the CPU 3400; a EEPROM (Electric Erasable Programmable Read Only Memory) 3403, in which is stored an accounting machine ID for the accounting machine 3455, a terminal ID and a telephone number for the accounting machine 3455 when used as a wireless telephone terminal, a merchant ID, a private key and a public key for a merchant digital signature, a service provider ID, and the telephone number and the public key of the service providing system 110 (the digital signature of the service provider accompanies the telephone number of the service providing system); a cryptographic processor 3404, which encrypts and decrypts data under the control of the CPU 3400; a data codec 3405, which encodes data to be transmitted and decodes received data under the control of the CPU 3400; an infrared communication module 3406, which transmits and receives infrared rays during infrared communication; a channel codec 3408, which generates data to be transmitted along a radio channel, and extracts, from received data, data that is addressed to the accounting machine 3455; a modulator 3409, which modulates a serial digital signal 3433 input by the channel codec 3408 to obtain an analog transmission signal 3435 that employs as a baseband an electric signal 3440 that is transmitted by a PLL 3412; a demodulator 3410, which demodulates a received analog signal 3436 while employing as a baseband an electric signal 3439 that is supplied by the PLL 3412, and which transmits a serial digital signal 3434 to the channel codec 3408; an RF unit 3411, which changes the analog transmission signal 3435 received from the modulator 3409 into a radio wave and outputs it through an antenna 701, and which, upon receiving a radio wave through the antenna 701, transmits an analog reception signal 3436 to the demodulator 3410; an external interface 3413, which serves as an interface for the sales mechanism 3456; and a control logic unit 3407, which activates the channel codec 3408, the PLL 3412 and the RF unit 3411, and which processes interrupt signals that are transmitted by the channel codec 3408 and the external interface 3413 and serves as an interface when the CPU 3400 accesses the channel codec 3408, the PLL 3412, the RF unit 3411 or the external interface 3413.

[1168] The sales mechanism 3456 comprises: a touch panel LCD 702; a loudspeaker 3415; a product selection switch 704; a sold out display 705; a price calculator 3416, for calculating the price of a product; a product manager 3417, for managing the products in stock; a product output mechanism 3418, for outputting a selected product to the discharge port 703; a CD-ROM drive 3419; and a controller 3414, for controlling the operations of the touch panel LCD 702, the loudspeaker 3415, the sold out display (LED) 705, the price calculator 3416, the product manager 3417, the product output mechanism 3418, and the CD-ROM drive 3419.

[1169] The accounting machine 3455 and the sales mechanism 3456 communicate with each other via the external interface 3413. The accounting machine 3455 receives an accounting process request from the sales mechanism 3456, and performs the payment card settlement process for a designated amount. The amount for the payment card settlement is calculated by the price calculator 3416 of the sales mechanism 3456. That is, the accounting device 3455 performs only the payment card settlement process, and the sales mechanism 3456 performs another process as an automatic vending machine.

[1170] The sales mechanism 3456 has two primary operating modes: a purchase mode and a product information mode. The purchase mode is the mode in which the purchase of a product by a user takes place, and the product information mode is a mode in which information concerning a product is provided to a user before (or after) the product has been purchased.

[1171] An operating menu and various information are displayed on the touch panel LCD 702 by the controller 3414. Normally, the operation menu shown in Fig. 7 is displayed on the touch panel LCD 702. When a user presses "purchase" ("purchase start operation"), the sales mechanism 3456 is set to the purchase mode. When a user presses "product information," the sales mechanism 3456 is set to the product information mode.

[1172] A CD-ROM on which information concerning products is stored is loaded into the CD-ROM drive 3419. When the user presses "product information" on the operating menu and the product information mode is set, the information stored on the CD-ROM is output to the touch panel LCD 702 and through the loudspeaker 3415.

[1173] The information concerning products that is stored on the CD-ROM is multimedia information including text, images, videos and audio, and may be video information consisting of a CF (Commercial Film) of a product. Especially for a packaged media product, such as a video or a music CD (Compact Disk), or a game software product, sample information for the product is stored on the CD-ROM so that the user can try out the product in the product information mode.

[1174] When the purchase mode is set by pressing "purchase" on the operating menu, the message "Select desired product" is displayed on the touch panel LCD (display "waiting for product selection operation"), and the sales mechanism enters the product selection operation waiting state. When the user depresses the product selection switch, the name, the volume and the total amount of the product, and a "payment" button indicating the start of the payment operation are displayed on the touch panel LCD (display "waiting for payment start operation"). At this time, the price calculator 3416 calculates the total amount, and the product manager 3417 verifies the count of the product in stock. This process is performed each time the user depresses the product selection switch. When the in stock supply of a product is exhausted, the sold out display (LED) blinks and the user can no longer select the pertinent product.

[1175] When the user depresses the "payment" button ("payment start operation"), the controller 3414 transmits, to the accounting machine 3455, an accounting processing request for an amount that corresponds to the total amount provided by the price calculator 3416, and displays, on the touch panel LCD, a message requesting the payment using an electronic payment card (display "waiting for payment operation").

[1176] When the payment card settlement process has been completed by the accounting machine 3455 and the mobile user terminal 100, the controller 3414 controls the product output mechanism 3418 so as to output a selected product at the discharge port 703, displays on the touch panel a message indicating the settlement process has been completed, and a little later, displays the operating menu again. At this time, the multimedia information stored on the CD-ROM may be output instead of the message indicating that the settlement has been completed.

[1177] The accounting machine 3455 performs the payment card settlement process that is requested by the sales mechanism 3456, and has partially the same arrangement as the merchant terminal 103. A difference from the merchant terminal 103 is that the accounting machine 3455 does not include a unit, such as an audio codec for performing audio processing, and input/output interfaces, such as number key switches, an execution switch, a bar code reader and an LCD, and instead, includes the external interface 3413 for communicating with the sales mechanism 3456.

[1178] In addition, as a functional difference, the accounting machine does not include the credit card settlement function and the digital wireless telephone communication function, which is employed for data communications with the service providing system.

[1179] The cryptographic processor 3404 includes a secret key encryption and decryption function and a public key encryption and decryption function. The cryptographic processor 3404 employs a cryptography method determined by the CPU 3400, and the keys to encrypt or decrypt data selected by the CPU 3400. The encryption and decryption functions of the cryptographic processor 3404 are employed to perform a digital signature process or a closing process for a message, and to decrypt a closed and encrypted message or to verify a digital signature accompanying a message.

[1180] The data codec 3405 encodes data to be transmitted or decodes data that was received, under the control of the CPU 3400. In this case, the encoding is a process for generating data to be transmitted that includes communication control information and error correction information, and the decoding is a process

for performing error correction for the received data and for removing extra communication control information in order to obtain the data that a sender was to originally transmit. The data codec 3405 has a function for encoding or decoding data during data communication conducted using a digital wireless telephone, and a function for encoding or decoding data during infrared communication. The data codec 3405 performs the encoding or decoding as determined by the CPU 3400 for data that are selected by the CPU 3400.

[1181] When, for example, a closed message accompanied by a digital signature is to be transmitted via digital wireless telephone communication, the CPU 3400 employs the cryptographic processor 3404 to perform a digital signature process and a closing process for a message, employs the data codec 3405 to encode the obtained message to provide a data communication form that is suitable for a digital wireless telephone, and transmits the resultant message through the control logic unit 3407 to the channel codec 3408.

[1182] When a closed message accompanied by a digital signature is received via digital wireless telephone communication, the CPU 3400 reads that message from the channel codec 3408 through the control logic unit 3407, employs the data codec 3405 to decode the received message, and permits the cryptographic processor 3404 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1183] Similarly, when a closed message accompanied by a digital signature is to be transmitted via infrared communication, the CPU 3400 employs the cryptographic processor 3404 to provide a digital signature for the message and to close the message, and employs the data codec 3405 to encode the obtained message to provide a data form that is suitable for infrared communication. Then, the resultant message is transmitted to the infrared communication module 3406.

[1184] When a closed message accompanied by a digital signature is received via infrared communication, the CPU 3400 reads that message from the infrared communication module 3406, employs the data codec 3405 to decode the received message, and permits the cryptographic processor 3404 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1185] The channel codec 3408 adds identification data, as header information, to data-communication data that are received as a digital signal 3429 from the CPU 3400 via the control logic unit 3407, then converts the data into a serial digital signal 3433 having a data format that is suitable for a digital wireless telephone, and transmits the signal 3433 to the modulator 3409.

[1186] In addition, upon receiving a serial digital signal 3434 from the demodulator 3410, the channel codec 3408 examines a terminal ID and extracts only such data as is addressed to the channel codec 3410, removes the communication control information for the digital wireless telephone, identifies the digital audio data and the data-communication data in the header information, and transmits the data-communication data as a digital audio signal 3429 to the audio codec 3012 and the control logic unit 3407.

[1187] Further, upon receiving a digital wireless call or data-communication data, the channel codec 3408 asserts an interrupt signal 3431. The interrupt signal 3431 is a signal requesting that the CPU 3400 perform the process for a digital wireless phone communication that has been received and a process for data-communication data.

[1188] In order to perform these processes, as is shown in Fig. 35A, the channel codec 3408 includes: an ID register (ID) 3505, in which is stored a terminal ID; a channel codec control register (CHCTL) 3506, which controls the operation of the channel codec 3408; a data transmission buffer 3507, in which are stored data-communication data received from the CPU 3400 via the control logic unit 3407; and a data reception buffer 3508, in which are stored data-communication data extracted from received data.

[1189] A control signal 3432 is a control signal with which the CPU 3400 directs the channel codec 3408 via the control logic unit 3407 in order to write data to the data transmission buffer 3507 and to read data from the data reception buffer 3508. When the control signal 3432 goes low, the data-communication data are written to the data transmission buffer 3507, and when the control signal 3432 goes high, the data-communication data are read from the data reception buffer 3508.

[1190] The modulator 3409 modulates a serial digital signal 3433 received from the channel codec 3408 to provide an analog transmission signal 3435, which is employed as a baseband for an electric signal 3440

that is supplied by the PLL 3412, and transmits the signal 3435 to the RF unit 3411. The analog transmission signal 3435 received by the RF unit 3411 is output as a radio wave through the antenna 701.

[1191] When a radio wave is received at the antenna 701, an analog reception signal 3436 is transmitted by the RF unit 3411 to the demodulator 3410. The demodulator 3410 demodulates the analog signal 3436, while employing as its baseband an electric signal 3439 that is supplied by the PLL 3412, and transmits an obtained serial digital signal 3434 to the channel codec 3408.

[1192] The external interface 3413 is an interface circuit for connecting the accounting machine 3455 to the sales mechanism 3456. An accounting process request is transmitted by the sales mechanism 3456 to the accounting machine 3455 during the interrupt process. The interrupt process is requested of the CPU 3400 when the external interface 3413 asserts an interrupt signal 3443.

[1193] The control logic unit 3407 includes five internal registers, as is shown in Fig. 35A: a frame counter (FRAMEC) 3500, a start frame register (FRAME) 3501, a clock counter (CLOCKC) 3502, an update time register (UPTIME) 3503, and an interrupt register (INT) 3504.

[1194] The frame counter 3500 is employed to count the number of frames for the digital wireless telephone; the start frame register 3501 is employed to store the frame number of the frame that is to be activated next; the clock counter 3502 is employed to measure the current time; the update time register 3503 is employed to store the time at which the automatic vending machine 104 will communicate with the service providing system 110 to update data in the RAM 3402 (data updating process); and the interrupt register 3504 is employed to indicate the type of interrupt that has been generated for the CPU 3400.

[1195] Generally, to receive a call, the digital wireless telephone intermittently acquires control data for a control channel and compares it with the terminal ID. The automatic vending machine 104 employs the frame counter 3500 and the start frame register 3501 to intermittently acquire control data. First, the frame number of the frame to be activated next is stored in advance in the start frame register 3501, and when the count held by the frame counter 3500 equals the count held by the start frame register 3501, the control logic unit 3407 activates the channel codec 3408, the PLL 3412 and the RF unit 3411 to receive control data.

[1196] When the count held by the clock counter 3502 matches the count held by the update time register 3503, or when the interrupt signal 3431 or 3443 is asserted, the control logic unit 3407 writes the type of and the reason for the interrupt in the interrupt register (INT) 3504, and asserts an interrupt signal 3428 requesting that the CPU 3400 perform an interrupt process. For the interrupt processing, the CPU 3400 reads the type of and the reason for the interrupt that are stored in the interrupt register (INT) 3504, and then performs a corresponding process.

[1197] The individual bit fields of the interrupt register (INT) 3504 are defined as is shown in Fig. 35B.

[1198] Bit 30 represents the digital wireless telephone communication state. When the bit value is 0, it indicates the state is one where no digital wireless telephone communication is being performed, and when the bit value is 1, it indicates the state is one where digital wireless telephone communication is in progress.

[1199] Bit 29 represents the generation of a frame interrupt requesting the intermittent acquisition of control data. When the bit value is 1, it indicates a condition that exists when a frame interruption has occurred. In this bit field, a 1 is set when the count held by the frame counter 3500 equals the count held by the start frame register 3501.

[1200] Bit 28 represents the generation of a call arrival interrupt. When the bit value is 1, it indicates that a digital wireless call has arrived. In this bit field, a 1 is set when the terminal ID is matched and the interrupt signal 3432 is asserted during the intermittent acquisition of control data for the digital wireless phone.

[1201] Bit 27 represents the generation of a data reception interrupt. When the bit value is 1, it indicates that data is being received. In this bit field, a 1 is set when the data-communication data are received and the interrupt signal 3431 is asserted during the course of digital wireless telephone communication.

[1202] Bit 26 represents the generation of an update interrupt requesting the performance of a data updating process. When the bit value is 1, it indicates the generation the update interrupt. In this bit field, a

1 is set when the count held by the clock counter 3502 matches the count held by the update time register 3503.

[1203] Bit 25 represents the generation of an external IF interrupt requesting data communication be initiated with the sales mechanism 3456. When the bit value is 1, it signals the generation of the external IF interrupt. In this bit field, a 1 is set when the interrupt signal 3443 received from the external interface 3413 is asserted.

[1204] Data stored in the RAM 3402 will now be described.

[1205] Fig. 36 is a specific diagram of a RAM map for data stored in the RAM 3402.

[1206] The RAM 3402 is constituted by four areas: a fundamental program object area 3600, a service data area 3601, a work area 3602 and a temporary area 3603. In the fundamental program object area 3600 are stored an upgraded module of a program stored in the ROM 3401, a patch program and an additional program. The work area 3602 is a work area that the CPU 100 employs when executing a program, and the temporary area 3603 is an area in which information received by the automatic vending machine is stored temporarily.

[1207] The service data area 3601 is an area in which are stored contract information for the electronic commerce service, available payment card information and history information, and the data in this area are managed by the service providing system. The service data area 3601 is constituted by seven sub-areas: a data management information area 3604, a merchant information area 3605, a merchant public key certificate area 3606, a merchant preference area 3607, an available payment card list 3608, a transaction list area 3609 and an object data area 3610.

[1208] The data management information area 3604 is an area in which is stored management information for data stored in the service data area 3601; the merchant information area 3605 is an area in which are stored the name of a merchant and information for the contents of a contract with a service provider; the merchant public key certificate area 3606 is an area in which a public key certificate for a merchant is stored; the merchant preference area 3607 is an area in which is stored preference information for a merchant that concerns the mobile electronic commerce service; the available payment card list area 3608 is an area in which is stored list information for those payment cards that the merchant can handle; the transaction list area 3609 is an area in which sales history information for the mobile electronic commerce service is stored; and the object data area 3610 is an area in which are stored object data for the information managed in the other six areas.

[1209] The information stored in the service data area 3601 will now be described in detail.

[1210] Fig. 37 is a detailed, specific diagram showing the relationships established for information stored in the service data area 3601.

[1211] The data management information 3604 consists of eight types of information: a last data update date 3700, a next data update date 3701, an accounting machine status 3702, a merchant information address 3703, a merchant public key certificate address 3704, a merchant preference address 3705, an available payment card list address 3706 and a transaction list address 3707.

[1212] The last data update date 3700 represents the date on which the service providing system 110 last updated the data in the RAM 3402, and the next data update date 3701 represents the date on which the service providing system 110 will next update the data in the service data area 3601. The automatic vending machine 104 automatically initiates an update process when the time set according to the next data update date 3701 is reached.

[1213] The time of the next data update date 3701 is set in the update time register 3503. When the next data update date 3701 is reached, the automatic vending machine 104 initiates the data updating process. During the data updating process, the service providing system 110 updates data stored in the RAM. This process is performed daily during a period (e.g., late at night) in which communication traffic is not very heavy. The data updating process will be described in detail later.

[1214] The accounting machine status 3702 represents the status of the accounting machine 3455. The merchant information address 3703, the merchant public key certificate address 3704, the merchant

preference address 3705, the available payment card list address 3706 and the transaction list address 3707 respectively represent the first addresses for the areas in which are stored the merchant information 3605, the merchant public key certificate 3606, the merchant preference information 3607, the available payment card list 3608 and the transaction list 3609.

[1215] The available payment card list 3608 includes list information for payment cards that can be handled by a merchant.

[1216] In the available payment card list 3608, for each payment card, seven types of information are entered: a card name 3708, a card code 3709, a payment card issuer ID 3710, a validity term 3711, an accounting machine private key 3712, a card public key 3713, and a payment card accounting module address 3714. The card name 3708 represents the name of a payment card that the merchant can handle; the card code 3709 is code information that represents the type of electronic payment card; the payment card issuer ID 3710 is ID information for a payment card issuer; and the validity term 3711 is the period during which the electronic payment card is valid. The accounting machine private key 3712 and the card public key 3713 are encryption keys that are respectively paired with the accounting machine public key 2012 and the card private key 2011 for the electronic payment card.

[1217] The payment card accounting module address 3714 is an address in the object data area 3610 in which is stored a program module (a payment card accounting module) for clearing the electronic payment card.

[1218] In accordance with the contract entered into by the merchant and the service providing system, the service providing system sets up or updates the contents of the available payment card list 3608 in the data updating process.

[1219] In the transaction list 3609, list information is stored to manage the history information for sales through the mobile electronic commerce service. For the sales effected through one payment card clearing process, in the transaction list 3609 are stored four information items: a transaction number 3715, a service code 3716, a transaction time 3717, and a transaction information address 3718.

[1220] The transaction number 3715 is a number uniquely identifying a transaction performed with a user (from the view of the merchant); the service code 3716 is code information identifying the type of mobile electronic commerce service that was provided for the user; and the transaction time 3717 is time information for the time at which a product was sold or the service was provided via the mobile electronic service.

[1221] The transaction information address 3718 is an address in the object data area 3610 at which is stored a micro-check that describes the contents of the sale and a receipt.

[1222] The internal structure of the electronic telephone card accounting machine 800 will now be described.

[1223] Fig. 38 is a block diagram illustrating the arrangement of the electronic telephone card accounting machine 800.

[1224] In Fig. 38, the electronic telephone card accounting machine 800 comprises: a CPU (Central Processing Unit) 3800, which employs a program stored in a ROM (Read Only Memory) 3801 to process data for transmission and for reception and to control the other components via a bus 3845; a RAM (Random Access Memory) 3802 and a hard disk 3803, whereat are stored data that have been processed and that are to be processed by the CPU 3800; a EEPROM (Electric Erasable Programmable Read Only Memory) 3804, in which is stored an accounting machine ID for the electronic telephone card accounting machine 800, a communication service provider ID, a private key and a public key for the digital signature of a communication service provider, a service provider ID, and the telephone number and the public key of the service providing system 110 (the digital signature of the service provider accompanies the telephone number of the service providing system); a cryptographic processor 3805, which encrypts and decrypts data under the control of the CPU 3800; a data codec 3806, which encodes data to be transmitted and decodes received data under the control of the CPU 3800; and an external interface 3807, which serves as an interface for the switch 801.

[1225] The electronic telephone card accounting machine 800 and the switch 801 communicate with each

other via the external interface 3807. The electronic telephone card accounting machine 800 receives an accounting process request from the switch 801 and performs the telephone card settlement process for a designated value. The value for the telephone card settlement is designated by the switch 801.

[1226] For a communication (micro-check call) using the electronic telephone card, upon receiving the accounting process request from the switch 801, the electronic telephone card accounting machine 800 exchanges settlement information with the mobile user terminal 100 upon the initiation of and during the line connection process (communication in process), and performs the telephone card settlement process. The switch 801 switches the lines in accordance with the condition of the settlement process performed by the electronic telephone card accounting machine 800.

[1227] Upon the initiation of the line connection process, and upon each occurrence of the elapse of a constant period of time, the telephone card settlement process is performed for the total communication charge assessed for the communication time.

[1228] First, when the line connection process is begun, a settlement is made for the communication charge V (V > 0) for a constant communication time T (T > 0). Then, on each occasion that the communication time exceeds T, a settlement process is performed for a communication charge 2V for a communication time 2T, instead of for a communication charge V. Thereafter, whenever the communication time exceeds NT (N is a natural number), a settlement process is performed for a communication charge (N + 1)V for a communication time (N + 1)T, rather than for a communication charge NV.

[1229] When the electronic telephone card accounting machine 800 has normally completed the telephone card settlement process for the received accounting process request, the switch 801 either establishes a new line connection, or continues the current line connection. When, for a specific reason, the telephone card settlement is not successful, the switch 801 either refrains from establishing a new line connection, or disconnects the line that is currently in use.

[1230] The cryptographic processor 3805 includes a secret key encryption and decryption function and a public key encryption and decryption function. The cryptographic processor 3805 employs a cryptography method determined by the CPU 3800 and the keys to encrypt or decrypt data selected by the CPU 3800. The encryption and decryption functions of the cryptographic processor 3805 are employed to perform a digital signature process or a closing process for a message, and to decrypt a closed and encrypted message or to verify a digital signature accompanying a message.

[1231] The data codec 3806 encodes data to be transmitted or decodes data that is received, under the control of the CPU 3800. In this case, the encoding is a process for generating data to be transmitted that includes communication control information and error correction information, and the decoding is a process for performing error correction for the received data and for removing extra communication control information in order to obtain the data that a sender was to originally transmit. The data codec 3806 has a function for encoding or decoding data during data communication conducted using a digital wireless telephone, and a function for encoding or decoding data during infrared communication. The data codec 2806 performs encoding or decoding determined by the CPU 3800 for data that are selected by the CPU 3800.

[1232] When, for example, a closed message accompanied by a digital signature is to be transmitted to the mobile user terminal 100, the CPU 3800 employs the cryptographic processor 3805 to perform a digital signature process and a closing process for a message, employs the data codec 3806 to encode the obtained message to provide a data communication form that is suitable for digital telephone communication, and transmits the resultant message through the external interface 3807 to the switch 801.

[1233] When a closed message accompanied by a digital signature is received from the mobile user terminal 100, the CPU 3800 receives that message through the external interface 3807, employs the data codec 3806 to decode the received message, and permits the cryptographic processor 2805 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1234] Similarly, when a closed message accompanied by a digital signature is to be transmitted to the service providing system 110, the CPU 3800 employs the cryptographic processor 3805 to provide a digital signature for the message and to close the message, and employs the data codec 3806 to encode the obtained message and produce a data form suitable for digital telephone communication. Then, the resultant message is transmitted through the external interface 3807 to the switch 801.

[1235] When a closed message accompanied by a digital signature is received from the service providing system 110, the CPU 3800 receives that message through the external interface 3807, employs the data codec 3806 to decode the received message, and permits the cryptographic processor 3805 to decrypt the closed and encrypted message and to verify the digital signature accompanying the message.

[1236] Data stored in the RAM 3802 will now be described.

[1237] Fig. 39 is a specific diagram of a RAM map for data stored in the RAM 3802.

[1238] The RAM 3802 is constituted by four areas: a fundamental program object area 3900, a service data area 3901, a work area 3902 and a temporary area 3903. In the fundamental program object area 3900 are stored an upgraded module of a program stored in the ROM 3801, a patch program and an additional program. The work area 3902 is a work area that the CPU 100 employs when executing a program, and the temporary area 3903 is an area in which information received by the electronic telephone accounting machine is stored temporarily.

[1239] The service data area 3901 is an area in which are stored contract information for the electronic commerce service, available telephone card information and history information, and the data in this area are managed by the service providing system. The service data area 3901 is constituted by six sub-areas: a data management information area 3904, a communication service provider information area 3905, a communication service provider's public key certificate area 3906, a communication service provider preference area 3907, an available telephone card list 3908 and a transaction list area 3909.

[1240] The data management information area 3904 is an area in which is stored management information for data stored in the service data area 3901; the communication service provider information area 3905 is an area in which are stored the name of a communication service provider and information for the contents of a contract with a service provider; the communication service provider public key certificate area 3906 is an area in which a public key certificate for a communication service provider is stored; the communication service provider preference area 3907 is an area in which is stored preference information concerning the mobile electronic commerce service for a communication service provider; the available telephone card list area 3908 is an area in which is stored list information for those telephone cards the communication service provider can handle; and the transaction list area 3909 is an area in which is stored accounting history information for communication performed (micro-check call) using an electronic telephone card.

[1241] The information stored in the service data area 3901 will now be described in detail.

[1242] Fig. 40 is a detailed, specific diagram showing the relationships established for information stored in the service data area 3901.

[1243] The data management information 3904 consists of eight types of information: a last data update date 4000, a next data update date 4001, an accounting machine status 4002, a communication service provider information address 4003, a communication service provider public key certificate address 4004, a communication service provider preference address 4005, an available telephone card list address 4006 and a transaction list address 4007.

[1244] The last data update date 4000 represents the date on which the service providing system 110 last updated the data in the RAM 3802 and on the hard disk 3803, and the next data update date 4001 represents the date on which the service providing system 110 will next update the data in the service data area 3901. The electronic telephone card accounting machine 800 automatically initiates an update process when the time set according to the next data update date 4001 is reached.

[1245] The accounting machine status 4002 represents the status of the electronic telephone card accounting machine 800. The communication service provider information address 4003, the communication service provider public key certificate address 4004, the communication service provider preference address 4005, the available telephone card list address 4006 and the transaction list address 4007 respectively represent the first addresses for the areas in which are stored the communication service provider information 3905, the communication service provider public key certificate 3906, the communication service provider preference information 3907, the available telephone card list 3908 and the transaction list 3909.

[1246] The available telephone card list 3908 includes list information for telephone cards that can be handled by a communication service provider.

[1247] In the available telephone card list 3908, for each telephone card, seven types of information are entered: a card name 4008, a card code 4009, a telephone card issuer ID 4010, a validity term 4011, an accounting machine private key 4012, a card public key 4013, and a telephone card accounting module address 4014. The card name 4008 represents the name of a telephone card that the communication service provider can handle; the card code 4009 is code information that represents the type of electronic telephone card; the telephone card issuer ID 4010 is ID information for a telephone card issuer; and the validity term 4011 is the period during which the electronic telephone card is valid. The accounting machine private key 4012 and the card public key 4013 are encryption keys that are respectively paired with the accounting machine public key 2012 and the card private key 2011 for the electronic telephone card.

[1248] The telephone card accounting module address 4014 is an address on the hard disk 3803 at which is stored a program module (a telephone card accounting module) for clearing the electronic telephone card.

[1249] In accordance with the contract entered into by the communication service provider and the service providing system, the service providing system sets up or updates the contents of the available telephone card list 3908 in the data updating process.

[1250] In the transaction list 3909, list information is stored to manage the history information for sales through the mobile electronic commerce service. For one communication (micro-check call) employing an electronic telephone card, in the transaction list 3909 are stored four information items: a transaction number 4015, a service code 4016, a transaction time 4017, and a transaction information address 4018.

[1251] The transaction number 4017 is a number uniquely identifying a transaction performed with a user (from the view of the communication service provider); the service code 4016 is code information identifying the type of mobile electronic commerce service (micro-check call) that was provided for the user; and the transaction time 4017 is time information for the time at which the telephone card clearing process was performed.

[1252] The transaction information address 4018 is an address on the hard disk 3803 at which is stored a telephone micro-check that describes the contents of the charge and a receipt.

[1253] An explanation will now be given for the digital signature process and the closing process performed by the mobile user terminal 100 when it generates a message to be transmitted to the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104, the switching center 105, or the service providing system 110.

[1254] Since the digital signature process and the closing process are also performed in the same manner by the gate terminal 101, the merchant terminals 102 and 103, the automatic vending machine 104, the switching center 105 and the service providing system 110, the identities of the characters in the following explanation are generalized by using the titles Mr. A and Mr. B, rather than the terms user, merchant and service provider.

[1255] In the digital signature processing, an electronic signature is provided for a message, while the characteristic of the cryptographic process is employed by using the public key, "a message encrypted using a private key is decrypted only by using a public key that corresponds to that private key."

[1256] Figs. 41A and 41B are a flowchart for the digital signature processing and a diagram for explaining it when a message (Message) is accompanied by the digital signature of Mr. A.

[1257] First, at step 4100, the CPU performs the hash function calculation for a message 4103, and generates a message digest 4104. Then, at step 4101, the CPU permits the cryptographic processor to encrypt the message digest 4104 using the private key of Mr. A, and to generate a digital signature 4105. At step 4102, the CPU adds the digital signature 4105 to the original message 4103. Through the above processing, the CPU generates a message 4106 accompanied by the digital signature of Mr. A.

[1258] Reference numeral 4106 in Fig. 41B denotes a message accompanied by the digital signature of Mr. A. Hereinafter, in the drawings, the message accompanied by the digital signature is shown as indicated by

4106.

[1259] The closing processing will now be described. In the closing process, the character of the cryptographic process using the public key, "a message encrypted using a private key is decrypted only by using a public key that corresponds to that private key," is employed to allow only a specific person to read the contents of the message.

[1260] Figs. 42A and 42B are a flowchart and a diagram for explaining the processing performed when closing a message that is accompanied by the digital signature of a Mr. A and when addressing it to a Mr. B, who is the recipient.

[1261] First, at step 4200, the CPU employs a random number function to generate a secret key 4204, which is a secret encryption key. Then, at step 4201, the CPU permits the cryptographic processor to encrypt the message 4106, which is accompanied by the digital signature, by using the private key 4204. At step 4202, the CPU permits the cryptographic processor to encrypt the secret key 4204 by using the public key of Mr. B, who is the recipient. At step 4203, the CPU adds the output 4206 produced at step 4202 to the output 4205 produced at step 4201. Through the above processing, the CPU generates a closed message 4207 that is addressed to Mr. B.

[1262] Reference numeral 4207 in Fig. 42B denotes a closed message addressed to Mr. B. Hereinafter, in the drawings, the closed message is shown as is illustrated by 4207.

[1263] An explanation will now be given for the processing performed to decrypt a closed and encrypted message, and the processing performed for the examination of a digital signature by the mobile user terminal 100, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104, the switching center 105 or the service providing system 110 when the message is received from the service providing system. In the following explanation, characters are also generalized.

[1264] Figs. 43A and 43B are a flowchart and a diagram for explaining the processing performed to decrypt a closed message addressed to Mr. B.

[1265] First, at step 4300, the CPU separates a closed message 4302 addressed to Mr. B into a portion 4303, wherein the secret key is encrypted using the public key of Mr. B, and a message portion 4304 that is encrypted using the secret key. The CPU permits the cryptographic processor to employ the private key of Mr. B to decrypt the portion 4303 wherein the secret key is encrypted using the public key of Mr. B, and to extract the secret key 4305. Then, at step 4301, the CPU permits the cryptographic processor to employ the secret key 4305 to decrypt the message portion 4304 that is encrypted using the secret key. Through the above processing, the closed message is decrypted.

[1266] The digital signature examination process will now be described.

[1267] Figs. 44A and 44B are a flowchart and a diagram for explaining the processing performed when an examination of made of the digital signature of Mr. A, the sender, that accompanies a message. First, at step 4400, the CPU performs a hash function calculation for the message portion (Message' 4403) in a message 4306 accompanied by a digital signature, and generates a message digest 4405. Then, at step 4401, the CPU permits the cryptographic processor to decrypt, using the public key of Mr. A, a digital signature 4404 accompanying the message 4306. At step 4402, the CPU compares the output 4405 at step 4400 with the output 4406 at step 4401. When the contents match, the CPU ascertains that the verification has been successful. When the contents do not match, the CPU ascertains that a verification error has occurred. Through the above processing, the digital signature examination process is performed.

[1268] The processing performed by the service providing system 110 will now be described.

[1269] The service providing system 110 communicates with the mobile user terminal 100, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104, the switching center 105, the transaction processing system 106, the ticket issuing system 107, the payment card issuing system 108 and the telephone card issuing system 109, and serves as an agent for a user, a merchant, a communication service provider, a transaction processor, a ticket issuer, a payment card issuer and a telephone card issuer while providing a mobile electronic commerce service for a user, a merchant and a communication service provider.

[1270] In Fig. 45 is shown the process architecture for the service providing system 110.

[1271] The service providing system 110 provides a mobile electronic commerce service through the coordinated performances of eight different processors: a user processor (UP) 4502, a merchant processor (MP) 4502, a transaction process processor (TPP) 4504, a ticket issuer processor (TIP) 4505, a payment card issuer processor (PCIP) 4506, a telephone card issuer processor (TCIP) 4507, a service director processor (SDP) 4501, and a service manager processor (SMP) 4500, all of which are generated in the service server 900.

[1272] In Fig. 45, the user processor 4502 has a one-to-one correspondence with the mobile user terminal 100, and serves as an interface for communication between the service providing system 110 and the mobile user terminal 100.

[1273] The merchant processor 4503 has a one-to-one correspondence with the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 or the switching center 105, and serves as an interface for communication between the service providing system 110 and the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 or the switching center 105.

[1274] The transaction process processor 4504 corresponds to the transaction processing system 106, and serves as an interface for communication between the service providing system 110 and the transaction processing system 106. The ticket issuing processor 4505 corresponds to the ticket issuing system 107, and serves as an interface for communication between the service providing system 110 and the ticket issuing system 107. The payment card issuing processor 4506 corresponds to the payment card issuing system 108, and serves as an interface for communication between the service providing system 110 and the payment card issuing system 108. The telephone card issuing processor 4507 corresponds to the telephone card issuing system 109, and serves as an interface for communication between the service providing system 110 and the telephone card issuing system 109.

[1275] The service director processor 4501 produces a mobile electronic commerce service by communicating with the user processor 4502, the merchant processor 4503, the transaction process processor 4504, the ticket issuer processor 4505, the payment card issuer processor 4506 and the telephone card issuer processor 4507. The service manager processor 4500 manages the user processor, the merchant processor, the transaction process processor, the ticket issuer processor, the payment card issuer processor and the telephone card issuer processor, and the service director processor in the system providing service 110. The meaning of the expression "produces a personal remote credit transaction service" will be described in detail later.

[1276] The service providing system 110 may simultaneously communicate with a plurality of mobile user terminals and a plurality of gate terminals, merchant terminals (102 or 103), automatic vending machines and switching centers, may simultaneously process a plurality of mobile electronic commerce services, or may simultaneously communicate with a plurality of transaction processing systems, ticket issuing systems, payment cared issuing systems or telephone card issuing systems in order to process a plurality of mobile electronic commerce services. Accordingly, in the service server 900 there may be a plurality of user processors, merchant processors, transaction process processors, ticket issuer processors, payment card issuer processors, telephone card issuer processors and service director processors. These processors are generated or deleted by the service manager processor.

[1277] When the service server 900 is constituted by a plurality of computers, the user processor, the merchant processor, the transaction process processor, the ticket issuer processor, the payment card issuer processor, the telephone card issuer processor and the service director processor are separately generated by the plurality of computers, so that the load imposed on an individual processor can be distributed among the computers.

[1278] A set of cooperative processors for providing a single mobile electronic commerce service is determined by the service manager processor and is composed of at least one processor selected from among the user, the merchant, the transaction, the ticket issuer, the payment card issuer and the telephone card issuer processors, plus one service director processor. The set of cooperating processes is called a process group.

[1279] First, the user process 4502 will be described.

[1280] The user process 4502 is a process for controlling communication with the mobile user terminal 100, for verifying users, for encrypting data to be transmitted to the mobile user terminal 100, for decrypting data received from the mobile user terminal 100, for examining the validity of the data received from the mobile user terminal 100, and for preforming a remote access process, a data updating process, a forcible data updating process and a data backup process for the mobile user terminal 100.

[1281] The user process 4502 is generated by the performance of the service manager processor 4500 when the service providing system 110 communicates with the mobile user terminal 100. In the service manager process 4500, one user process 4502 is generated for one mobile user terminal 100 that is communicating with the service providing system 110.

[1282] In the user process 4502, permission is provided only for the accessing of attribute information for the owner (the user) of the mobile user terminal 100, which is managed by the user information server 902, and data stored in the RAM 1502 of the mobile user terminal 100. In other words, other information can not be accessed during the performance of the user process 4502.

[1283] One mobile user terminal 100 corresponds to one user process 4502, and the user process 4502 can effectively engage only its corresponding mobile user terminal 100; it can not communicate directly with another mobile user terminal.

[1284] The merchant process 4503 will now be described.

[1285] The merchant process is a process for controlling communication with the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105, for verifying a merchant, for encrypting data to be transmitted to the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105, for decrypting data received from the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105, for examining the validity of the data received from the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105, for preforming a data updating process or a forcible data updating process for the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105, for performing a remote access process for the gate terminal 101, the merchant terminal 102 and the merchant 103, and for performing a data backup process for the merchant terminal 103.

[1286] The merchant process 4503 is generated by the performance of the service manager process 4500 when the service providing system 110 communicates with the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105. In the service manager process 4500, one merchant process 4503 is generated for a gate terminal 101, a merchant terminal 102, a merchant terminal 103, an automatic vending machine 104 or a switching center 105 that communicates with the service providing system 110.

[1287] In the merchant process 4503, permission is provided only for the accessing of the attribute information for the merchant and the communication service provider, which are managed by the merchant information server 903, and data in the RAM and on the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 and the switching center 105. In other words, other information can not be accessed during the performance of the merchant process 4503.

[1288] One gate terminal 101, one merchant terminal 102, one merchant terminal 103, one automatic vending machine 104 or one switching center 105 corresponds to one merchant process 4503, and the merchant process 4503 is effective only for a corresponding gate terminal 101, merchant terminal 102, merchant terminal 103, automatic vending machine or switching center 105; it can not communicate directly with another credit gate terminal, merchant terminal (102, 103), automatic vending machine or switching terminal.

[1289] The transaction processor process 4504 will now be described.

[1290] The transaction processor process is a process for controlling communication with the transaction processing system 106, for verifying a transaction processor, for encrypting data to be transmitted to the

transaction processing system 106, for decrypting data received from the transaction processing system 106, and for examining the validity of the data received from the transaction processing system 106.

[1291] The transaction processor process 4504 is generated by the service manager processor 4500 when the service providing system 110 communicates with the transaction processing system 106. One transaction processor process 4504 is generated to control communication across one communication line between the service providing system 110 and the transaction processing system 106. The digital communication line 131 linking the service providing system 110 and the transaction processing system 106 is multiplexed so that it can serve as a plurality of communication lines. To perform communication between the service providing system 110 and the transaction processing system 106 across a plurality of communication lines during the same period, the service manager process 4500 generates multiple transaction processor processes 4504 that are equivalent in number to the communication lines.

[1292] In a transaction processor process 4504, permission is provided only for the accessing of the attribute information and transaction history information for the transaction processor in an area wherein is installed the transaction processing system 106 that is managed by the transaction processor information server 904. In other words, other information can not be accessed during the performance of the transaction processor process 4504.

[1293] The transaction processor process 4504 is effective only when employed with a corresponding transaction processing system 106, and can not communicate directly with another transaction processing system.

[1294] The ticket issuer process 4505 will now be described.

[1295] The ticket issuer process is a process for controlling communication with the ticket issuing system 107, for verifying a ticket issuer, for encrypting data to be transmitted to the ticket issuing system 107, for decrypting data received from the ticket issuing system 107, and for examining the validity of the data received from the ticket issuing system 107.

[1296] The ticket issuer process 4505 is generated by the service manager processor 4500 when the service providing system 110 communicates with the ticket issuing system 107. One ticket issuer process 4505 is generated to control communication across one communication line between the service providing system 110 and the ticket issuing system 107. The digital communication line 132 linking the service providing system 110 and the ticket issuing system 107 is multiplexed so that it can serve as a plurality of communication lines. To perform communication between the service providing system 110 and the ticket issuing system 107 across a plurality of communication lines during the same period, the service manager process 4500 generates multiple ticket issuer processes 4505 that are equivalent in number to the communication lines.

[1297] In the ticket issuer process 4505, permission is provided only for the accessing of attribute information and ticket issuance history information by the ticket issuer in the area wherein is installed the ticket issuing system 107 that is managed by the ticket issuer information server 905. In other words, other information can not be accessed during the performance of the ticket issuer process 4505.

[1298] The ticket issuer process 4505 is effective only when employed with a corresponding ticket issuing system 107, and can not communicate directly with another ticket issuing system.

[1299] The payment card issuer process 4506 will now be described.

[1300] The payment card issuer process is a process for controlling communication with the payment card issuing system 108, for verifying a payment card issuer, for encrypting data to be transmitted to the payment card issuing system 108, for decrypting data received from the payment card issuing system 108, and for examining the validity of the data received from the payment card issuing system 108.

[1301] The payment card issuer process 4506 is generated by the service manager processor 4500 when the service providing system 110 communicates with the payment card issuing system 108. One payment card issuer process 4506 is generated to control communication across one communication line between the service providing system 110 and the payment card issuing system 108. The digital communication line 133 linking the service providing system 110 and the payment card issuing system 108 is multiplexed so that it can serve as a plurality of communication lines. To perform communication between the service

providing system 110 and the payment card issuing system 108 across a plurality of communication lines during the same period, the service manager process 4500 generates multiple payment card issuer processes 4506 that are equivalent in number to the communication lines.

[1302] In the payment card issuer process 4506, permission is provided only for the accessing of the attribute information and payment card issuance history information by the payment card issuer in the area wherein is installed the payment card issuing system 108 that is managed by the payment card issuer information server 906. In other words, other information can not be accessed during the performance of the payment card issuer process 4506.

[1303] The payment card issuer process 4506 is effective only when employed with a corresponding payment card issuing system 108, and can not communicate directly with another payment card issuing system.

[1304] The telephone card issuer process 4507 will now,be described.

[1305] The telephone card issuer process is a process for controlling communication with the telephone card issuing system 109, for verifying a telephone card issuer, for encrypting data to be transmitted to the telephone card issuing system 109, for decrypting data received from the telephone card issuing system 109, and for examining the validity of the data received from the telephone card issuing system 109.

[1306] The telephone card issuer process 4507 is generated by the service manager processor 4500 when the service providing system 110 communicates with the telephone card issuing system 109. One telephone card issuer process 4507 is generated to control communication across one communication line between the service providing system 110 and the telephone card issuing system 109. The digital communication line 134 linking the service providing system 110 and the telephone card issuing system 109 is multiplexed to serve as a plurality of communication lines. To perform communication between the service providing system 110 and the telephone card issuing system 109 across a plurality of communication lines during the same period, the service manager process 4500 generates multiple telephone card issuer processes 4507 that are equivalent in number to the communication lines.

[1307] In the telephone card issuer process 4507, permission is provided only for the accessing of the attribute information and the telephone card issuance history information for the telephone card issuer in the area wherein is installed the telephone card issuing system 109 that is managed by the telephone card issuer information server 907. In other words, other information can not be accessed during the performance of the telephone card issuer process 4507. The telephone card issuer process 4507 is effective only when employed with a corresponding telephone card issuing system 109, and can not communicate directly with another telephone card issuing system.

[1308] The service director process 4501 will now be described.

[1309] The service director process is a process for communicating with the user process, the merchant process and the transaction processor process that belong to the same group, and for producing the mobile electronic commerce service. The expression "producing the mobile electronic commerce service" means that the service director process cooperates with the other member processes in the same process group, and takes the initiative in performing the processing for the mobile electronic commerce service.

[1310] The service director processor 4501 is generated by the service manager process 4500 when the service providing system 110 performs various processes for a mobile electronic commerce service. A specified processing sequence is employed for the individual processes for performing the mobile electronic commerce service. In accordance with the processing sequence, a message received by the performance of a member process in the same group is handled, and a message requesting a process to be performed is transmitted to each member process. Upon receiving the message via the service director process 4501, a member process performs a corresponding process. Since the service director process cooperates with the other member processes in the same group, the processing for the electronic mobile commerce service can be performed.

[1311] To purchase an electronic ticket, the service director process, the user process, the ticket issuer process and the transaction processor process are assembled into one process group. To purchase an electronic payment card, the service director process, the user process, the payment card issuer process and the transaction processor process are assembled into one process group. And to purchase an

electronic telephone card, the service director process, the user process, the telephone card issuer process and the transaction processor process are assembled into one process group.

[1312] In the service director process 4501, permission is provided only for the accessing of the information that is managed by the service director information server 901, and information that a member process in the same group is permitted to access. In other words, other information can not be accessed during the performance of the service director process 4501.

[1313] The service manager process 4500 will now be described.

[1314] The service manager process is a process for generating or deleting the user process 4502, the merchant process 4503, the transaction processor process 4504, the ticket issuer process 4505, the payment card issuer process 4505, the telephone card issuer process 4505 and the service director process 4501, and for generating or deleting a process group.

[1315] The service manager process 4500 is always activated when the service providing system provides the mobile electronic commerce service. The generation and deletion of the service manager process is controlled by the management system 407.

[1316] In the service manager process 4500, permission is provided only for the accessing of information that is managed by the service director information server 901.

[1317] In other words, other information can not be accessed during the performance of the service manager process 4500.

[1318] The information stored in the user information server 902 of the service providing system 110 will now be explained.

[1319] The user information server 902 manages the user attribute information and the data in the RAM 1502 of the mobile user terminal 100.

[1320] Fig. 46 is a specific diagram showing information stored for each user in the user information server 902.

[1321] The user information server 902 stores 14 types of information for each user: user data management information 4600, personal information 4601, portrait image data 4602, a user public key certificate 4603, a terminal property 4604, user preference 4605, access control information 4606, terminal data 4607, telephony information 4608, a credit card list 4609, a ticket list 4610, a payment card list 4611, a telephone card list 4612, and a use list 4613.

[1322] The user data management information 4600 is management information for data to be stored for each user in the user information server 902.

[1323] The personal information 4601 is information concerning a user, such as the age, the date of birth, the occupation, the account number and the terms of a contract, and one part of this information corresponds to the personal information 1706 of the mobile user terminal 100.

[1324] The portrait image data 4602 are data for the portrait of a user; the user public key certificate 4603 is a certificate for the public key of a user; and the terminal property 4604 is attribute information for the mobile user terminal 100, such as the model number of the mobile user terminal 100, the serial number, the memory capacity of a RAM and the version of a stored program.

[1325] The user preference 4605 is preference information concerning the mobile electronic commerce service, and corresponds to the user preference 1709 in the mobile user terminal 100.

[1326] The access control information 4606 is information set by the user concerning the access control for user information and associated information; the terminal data 4607 are data in the RAM 1502 in the mobile user terminal 100; the telephony information 4608 is information concerning a digital wireless telephone, and corresponds to the telephony information 1710 of the mobile user terminal 100.

[1327] The credit card list 4609 is list information for credit cards registered by a user; the ticket list 4610 is

list information for electronic tickets owned by a user; the payment card list 4611 is list information for payment cards owned by a user; the telephone card list 4612 is list information for electronic telephone cards owned by a user; and the use list 4613 is use history information for the mobile electronic commerce service.

[1328] The user data management information 4600 consists of 18 types of information: a user name 4614, a user ID 4615, a user status 4616, a personal information address 4617, a portrait image data address 4618, a user public key certificate address 4619, a terminal property address 4620, a user preference address 4621, an access control information address 4622, a last update date 4623, a next update date 4624, a terminal data address 4625, a telephony information address 4626, a credit card list address 4627, a ticket list address 4628, a payment card list address 4629, a telephone card list address 4630, and a use list address 4631.

[1329] The user status 4616 indicates the status of the mobile user terminal 100, and corresponds to the terminal status 1802 of the mobile user terminal 100. The last update date 4623 provides the last date on which the data in the service data area 1701 of the mobile user terminal 100 were updated; and the next update date 4624 provides the date on which the data in the service data area 1701 will be updated next. These dates correspond to the last update date 1800 and the next update date 1801 of the mobile user terminal 100.

[1330] The personal information address 4617, the portrait image data address 4618, the user public key certificate address 4619, the terminal property address 4620, the user preference address 4621, the access control information address 4622, the terminal data address 4625, the telephony information address 4626, the credit card list address 4627, the ticket list address 4628, the payment card list address 4629, the telephone card list address 4630, and the use list address 4631 describe addresses in the user information server 902 at which are respectively stored the personal information 4601, the portrait image data 4602, the user public key certificate 4603, the terminal property 4604, the user preference 4605, the access control information 4605, the terminal data 4607, the telephony information 4608, the credit card list 4609, the ticket list 4610, the payment card list 4611, the telephone card list 4612, and the use list 4613.

[1331] The terminal data 4607 are data stored in the RAM 1502 of the mobile user terminal 100 when the updating process was previously performed, and are used for data comparison during the next data updating process and are also employed as backup data.

[1332] The credit card list 4609, the ticket list 4610, the payment card list 4611, the telephone card list 4612 and the use list 4613 correspond to the credit card list 1711, the ticket list 1712, the payment card list 1713, the telephone card list 1714 and the use list 1715 of the mobile user terminal 100. An object data address 4623, an electronic ticket address 4648, an electronic payment card address 4654, an electronic telephone card address 4660 and a user information address 4665 are addresses in the user information server 902.

[1333] The information stored in the merchant information server 903 of the service providing system 110 will now be explained.

[1334] The merchant information server 903 manages attribute information for a merchant or a communication service provider, and data stored in the RAMs and on the hard disks of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 (accounting machine 3455) and the switching center 105 (electronic telephone card accounting machine 800).

[1335] Fig. 47 is a specific diagram showing information stored for each merchant in the merchant information server 903.

[1336] For each gate terminal 101, each merchant terminal 102, each merchant terminal 103, each automatic vending machine 104 (accounting machine 3455) or each switching center 105 (electronic telephone card accounting machine 800), the merchant information server 903 stores 14 types of information: merchant data management information 4700, merchant information 4701, a public key certificate 4702, a system property 4703, merchant preference 4704, memory data 4705, disk data 4706, telephony information 4707, an available credit card list 4708, an available payment card list 4709, an available telephone card list 4710, a ticket list 4711, a transaction list 4712, and an authorization report list 4713.

[1337] The merchant data management information 4700 is management information for data to be stored in the merchant information server 903 for each gate terminal 101, each merchant terminal 102, each merchant terminal 103, each automatic vending machine 104 (accounting machine 3455) or each switching center 105 (electronic telephone card accounting machine 800).

[1338] The merchant information 4701 is information concerning a merchant or a communication service provider, such as an address, an account number and the terms of a contract, and one part of this information corresponds to the merchant information in the gate terminal 101, the merchant terminal 102, the merchant terminal 103 or the automatic vending machine 104 (accounting machine 3455), or the communication service provider information 4005 in the switching center 105 (electronic telephone accounting machine 800).

[1339] The public key certificate 4702 is a certificate for the public key of the merchant or the communication service provider; and the system property 4703 is attribute information for the gate terminal 101, the merchant terminal 102, the merchant terminal 103 or the automatic vending machine 104 (accounting machine 3455), or the switching center 105 (electronic telephone accounting machine 800), such as a model number, a serial number, the memory capacity of a RAM, the memory capacity of a hard disk, and the version of a stored program.

[1340] The merchant preference 4704 is preference information concerning a merchant or a communication service provider for the mobile electronic commerce service, and corresponds to the merchant preference in the gate terminal 101, the merchant terminal 102, the merchant terminal 103 or the automatic vending machine 104 (accounting machine 3455), or the communication service provider information 3906 in the switching center 105 (electronic telephone accounting machine 800).

[1341] The memory data 4705 are data in the RAM of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 (accounting machine 3455) or the switching center 105 (electronic telephone accounting machine 800), or data on a hard disk in the merchant terminal 102 or the switching center 105 (electronic telephone card accounting deice 800).

[1342] The telephony information 4707 is information concerning a digital telephone and a digital wireless telephone, and corresponds to the telephony information 2808 of the merchant terminal 102 or the telephony information 3208 of the merchant terminal 103.

[1343] The available credit card list 4708 is list information for those credit cards the merchant can handle; the available payment card list 4709 is list information for those payment cards the merchant can handle; the available telephone card list 4710 is list information for those telephone cards the merchant can handle; and the ticket list 4711 is list information for those electronic tickets the merchant sets up as tickets to be examined.

[1344] The transaction list 4712 is history information for the mobile electronic commerce service. The authorization report list 4713 is a list of authorizations for the electronic payment card, the electronic telephone card and the electronic ticket.

[1345] The merchant data management information 4700 consists of 19 types of information: a merchant name (or communication service provider name) 4714, a merchant ID (communication service provider ID) 4715, an accounting machine ID (gate ID) 4716, a merchant status 4717, a merchant information address 4718, a merchant public key certificate address 4719, a system property address 4720, a merchant preference address 4721, a last update date 4722, a next update date 4723, a memory data address 4724, a disk data address 4725, a telephony information address 4726, an available credit card list address 4727, an available payment card address 4728, an available telephone card address 4729, a ticket list address 4730, a transaction list address 4731, and an authorization report list address 4732.

[1346] The merchant status 4717 indicates the status of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 (accounting machine 3455) or the switching center 105 (electronic telephone accounting machine 800), and corresponds to the terminal status of the gate terminal 101, the merchant terminal 102 or the merchant terminal 103, or the accounting machine status of the automatic vending machine 104 (accounting machine 3455) or the switching center 105 (electronic telephone card accounting machine 800).

[1347] The last update date 4722 provides the last date on which the data in the service data area were

updated; and the next update date 4723 provides the date on which the data in the service data area will be updated next. These dates correspond to the last update date and the next update date of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 (accounting machine 3455) or the switching center 105 (electronic telephone accounting machine 800).

[1348] The merchant information address 4718, the public key certificate address 4719, the system property address 4720, the merchant preference address 4721, the memory data address 4724, the telephony information address 4726, the available credit card list address 4727, the available payment card list address 4728, the available telephone card list address 4729, the ticket list address 4730, the transaction list address 4731 and the authorization report list address 4732 indicate addresses in the merchant information server 903 at which are stored respectively the merchant information 4701, the public key certificate 4702, the system property 4703, the merchant preference 4704, the memory data 4705, the disk data 4706, the telephony information 4707, the credit card list 4708, the payment card list 4709, the telephone card list 4710, the ticket list 4711, the transaction list 4712 and the authorization report list 4713.

[1349] The available credit card list 4708, the available payment card list 4709, the available telephone card list 4710, the ticket list 4711, the transaction list 4712 and the authorization report list 4713 correspond to the credit card list, the payment card list, the telephone card list 3908, the ticket list 2409, the transaction list and the authorization report list of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the automatic vending machine 104 (accounting machine 3455) or the switching center 105 (electronic telephone accounting machine 800). The service code list address, the credit card clearing program address, the payment card clearing module address, the telephone card clearing program address, the ticket examination module address, the transaction information address and the authorization report address indicate those in the merchant information server 903.

[1350] The information stored in the transaction processor information server 904 of the service providing system 110 will now be explained.

[1351] The transaction processor information server 904 manages attribute information for the transaction processor and the transaction history information.

[1352] Fig. 48 is a specific diagram showing information stored for each transaction processor in the transaction processor information server 904.

[1353] The transaction processor information server 904 stores five types of information for each transaction processor: transaction processor data management information 4800, transaction processor information 4801, a transaction processor public key certificate 4802, an available credit card list 4803 and a clearing list 4804.

*[1354] The transaction processor data management information 4800 is management information for data to be stored for each transaction processor in the transaction processor information server 904. The transaction processor information 4801 is information concerning a transaction processor, such as an address, an account number and the terms of a contract; the transaction processor public key certificate 4802 is a certificate for the public key of the transaction processor; the available credit card list 4803 is list information for credit cards the transaction processor can handle; and the clearing list 4804 is clearing history information for the mobile electronic commerce service.

[1355] The transaction processor data management information 4800 consists of seven types of information: a transaction processor name 4805, a transaction processor ID 4806, a transaction processor status 4807, a transaction processor information address 4808, a transaction processor public key certificate address 4809, an available credit card list address 4811 and a clearing list address 4811.

[1356] The transaction processor status 4807 provides the service status in the settlement process of the transaction processing system 106. The transaction processor information address 4808, the transaction processor public key certificate address 4809, the available credit card list address 4810 and the clearing list address 4811 provide the addresses in the transaction processor information server 904 at which respectively are stored the transaction processor information 4801, the transaction processor public key certificate 4802, the credit card list 4803 and the clearing list 4804.

[1357] In the available credit card list 3102, two types of information are entered for each credit card: a

credit card name 4812 and a service code list address 4813.

[1358] The credit card name 4812 represents the name of a credit card that the transaction processor can handle, and the service code list address 4813 is an address of the transaction processor information server 904 at which is stored a service code list that shows the types of services that can be provided by the transaction processor when the credit card is used.

[1359] In the clearing list 4803, four types of information are stored for clearing one credit transaction service: a clearing number 4814, a service code 4815, a clearing time 4816, and a clearing information address 4817.

[1360] The clearing number 4814 uniquely represents the credit card clearing process, and the service code 4815 is a code number that describes the type of credit card service that is provided for the user The clearing time 4816 is the time at which the credit transaction service is cleared, and the clearing information address 4817 is an address of the transaction processor information server 904 at which is stored a clearing completion notification issued by the transaction processing system 106.

[1361] The information stored in the ticket issuer information server 905 of the service providing system 110 will now be explained.

[1362] The ticket issuer information server 905 manages the attribute information for the ticket issuer and the ticket issuing history information.

[1363] Fig. 49 is a specific diagram showing information stored in the ticket issuer information server 905 for each ticket issuer.

[1364] The ticket issuer information server 905 stores eight types of information for each ticket issuer: ticket issuer data management information 4900, ticket issuer information 4901, a ticket issuer public key certificate 4902, a service code list 4903, an installation card list 4904, an electronic ticket template list 4905, a transaction list 4906, and a usage report list 4907.

[1365] The ticket issuer data management information 4900 is management information for data for each ticket issuer that is to be stored in the ticket issuer information server 905; the ticket issuer information 4901 is information concerning a ticket issuer, such as an address, an account number and the terms of a contract; the ticket issuer public key certificate 4902 is a certificate for the public key belonging to a ticket issuer; the service code list 4903 is a list of service codes indicating the type of service provided by a ticket issuer; the installation card list 4904 is list information for the installation card numbers of electronic ticket installation cards issued by a ticket issuer; the electronic ticket template list 4905 is management information for a template program for an electronic ticket that corresponds to a ticket issued by a ticket issuer; the transaction list 4906 is ticket issuing history information for a ticket issuer; and the usage report list 4907 is management information for a usage report that the service providing system 110 issued the ticket issuing system 107.

[1366] The ticket issuer data management information 4900 consists of ten types of information: a ticket issuer processor name 4908, a ticket issuer ID 4909, a ticket issuer status 4910, a ticket issuer information address 4911, a ticket issuer public key certificate address 4912, a service code list address 4913, an installation card list address 4914, an electronic ticket template list address 4915, a transaction list address 4916 and a usage report list address 4917.

[1367] The ticket issuer status 4910 specifies the service status in the settlement process of the ticket issuing system 107. The ticket issuer information address 4911, the ticket issuer public key certificate address 4912, the service code list address 4913, the installation card list address 4914, the electronic ticket template list address 4915, the transaction list address 4916 and the usage report list address 4917 represent addresses in the ticket issuer information server 905 at which respectively are stored the ticket issuer information 4901, the ticket issuer public key certificate 4902, the service code list 4903, the installation card list 4904, the electronic ticket template list 4905, the transaction list 4906 or the usage report list 4907.

[1368] The electronic ticket template program is a model for an electronic ticket issued by the service providing system, and is registered in advance in the ticket issuer information server 905 in accordance with the contract entered into by the ticket issuer and the service provider. To issue an electronic ticket, the

service providing system employs the template program designated by the ticket issuing system to generate an electronic ticket, and transmits the ticket to the mobile user terminal.

[1369] The electronic template list 4905 includes five information items for one type of electronic ticket template program: a template code 4918, a transaction module address 4919, a representation module address 4920, a default representative component address 4921, and a ticket examination module address 4922.

[1370] The template code 4918 is code information describing the type of electronic ticket template program. The transaction module address 4919 is an address in the ticket issuer information server 905 at which is stored a program module that is the transaction module 1930 for an electronic ticket that is generated. The representation module address 4920 is an address in the ticket issuer information server 905 at which is stored a program module that is the representation module 1931 for an electronic ticket that is generated. The default representative component address 4921 is an address in the ticket issuer information server 905 at which default information is stored. The ticket examination module address 4922 is an address in the ticket issuer information server 905 at which is stored a ticket examination module for examining an electronic ticket that is generated. And the ticket examination module is a program module that corresponds to the transaction module.

[1371] The electronic ticket issuing commission 4903, which is a message by which the ticket issuing system requests that the service providing system request the issuance of an electronic ticket, includes not only ticket information, such as the date of an event and a seat number, but also a template code that specifies a template program and representative component information. The service providing system generates an electronic ticket using the transaction module and the representation module specified by the template code, and the representative component information that is included in the electronic ticket issuing commission.

[1372] Before the template program is registered in the ticket issuer information server 905, the operation and the safety of the mobile electronic commerce system are confirmed. Since several template programs are stored in advance, the ticket issuer can safely issue a ticket that performs various operations, as well as tickets of various designs. The procedures for issuing an electronic ticket will be described in detail later.

[1373] The transaction list 4906 includes four types of information for one ticket order or one ticket purchase: a transaction number 4923, a service code 4924, a transaction time 4925, and a transaction information address 4926.

[1374] The transaction number 4923 uniquely represents the ticket order process and the ticket purchase process; the service code 4924 represents the type of service provided by the ticket issuing system; the transaction time 4925 represents the time at which the ticket order process or the ticket purchase process was performed; and the transaction information address 4926 is an address in the ticket issuer information server 905 at which is stored a ticket order response or a receipt that was issued by the ticket issuing system 107.

[1375] The usage report list 4907 is management information for the usage report 7100 that the service providing system 110 issued to the ticket issuing system 107, and comprises a list of the usage report addresses 4927 that are located in the ticket issuer information server 905 in which the usage reports are stored.

[1376] The information stored in the payment card information server 905 of the service providing system 110 will now be explained.

[1377] The transaction processor information server 904 manages attribute information for the transaction processor and the transaction history information.

[1378] The information stored in the payment card issuer information server 906 of the service providing system 110 will now be explained.

[1379] The payment card issuer information server 906 manages the attribute information for the payment card issuer and the payment card issuing history information.

[1380] Fig. 50 is a specific diagram showing information stored in the payment card issuer information

server 906 for each payment card issuer.

[1381] The payment card issuer information server 906 stores eight types of information for each payment card issuer: payment card issuer data management information 5000, payment card issuer information 5001, a payment card issuer public key certificate 5002, a service code list 5003, an installation card list 5004, an electronic payment card template list 5005, a transaction list 5006, and a usage report list 5007.

[1382] The payment card issuer data management information 5000 is management information for data for each payment card issuer that is to be stored in the payment card issuer information server 906; the payment card issuer information 5001 is information concerning a payment card issuer, such as an address, an account number and the terms of a contract; the payment card issuer public key certificate 5002 is a certificate for the public key belonging to a payment card issuer; the service code list 5003 is a list of service codes indicating the type of service provided by a payment card issuer; the installation card list 5004 is list information for the installation card numbers of electronic payment card installation cards issued by a payment card issuer; the electronic payment card template list 5005 is management information for a template program for an electronic payment card that corresponds to a payment card issued by a payment card issuer; the transaction list 5006 is payment card issuing history information for a payment card issuer; and the usage report list 5007 is management information for a usage report that the service providing system 110 issued the payment card issuing system 108.

[1383] The payment card issuer data management information 5000 consists of ten types of information: a payment card issuer processor name 5008, a payment card issuer ID 5009, a payment card issuer status 5010, a payment card issuer information address 5011, a payment card issuer public key certificate address 5012, a service code list address 5013, an installation card list address 5014, an electronic payment card template list address 5015, a transaction list address 5016 and a usage report list address 5017.

[1384] The payment card issuer status 5010 specifies the service status in the issuance process of the payment card issuing system 108. The payment card issuer information address 5011, the payment card issuer public key certificate address 5012, the service code list address 5013, the installation card list address 5014, the electronic payment card template list address 5015, the transaction list address 5016 and the usage report list address 5017 represent addresses in the payment card issuer information server 906 at which respectively are stored the payment card issuer information 5001, the payment card issuer public key certificate 5002, the service code list 5003, the installation card list 5004, the electronic payment card template list 5005, the transaction list 5006 or the usage report list 5007.

[1385] The electronic payment card template program is a model for an electronic payment card issued by the service providing system, and is registered in advance in the payment card issuer information server 906 in accordance with the contract entered into by the payment card issuer and the service provider. To issue an electronic payment card, the service providing system employs the template program designated by the payment card issuing system to generate an electronic payment card, and transmits the payment card to the mobile user terminal.

[1386] The electronic template list 5005 includes five information items for one type of electronic payment card template program: a template code 5018, a transaction module address 5019, a representation module address 5020, a default representative component address 5021, and a payment card clearing module address 5022.

[1387] The template code 5018 is code information describing the type of electronic payment card template program. The transaction module address 5019 is an address in the payment card issuer information server 906 at which is stored a program module that is the transaction module 2030 for an electronic payment card that is generated. The representation module address 5020 is an address in the payment card issuer information server 906 at which is stored a program module that is the representation module 2031 for an electronic payment card that is generated. The default representative component address 5021 is an address in the payment card issuer information server 906 at which default information is stored. The payment card clearing module address 5022 is an address in the payment card issuer information server 906 at which is stored a payment card clearing module for clearing an electronic payment card that is generated. And the payment card clearing module is a program module that corresponds to the transaction module.

[1388] The electronic payment card issuing commission 6203, which is a message by which the payment

card issuing system requests that the service providing system request the issuance of an electronic payment card, includes not only payment card information, such as the face value of the payment card that is issued and the usage condition, but also a template code that specifies a template program and representative component information. The service providing system generates an electronic payment card using the transaction module and the representation module specified by the template code, and the representative component information that is included in the electronic payment card issuing commission.

[1389] Before the template program is registered in the payment card issuer information server 906, the operation and the safety of the mobile electronic commerce system are confirmed. Since several template programs are stored in advance, the payment card issuer can safely issue a payment card that performs various operations, as well as payment cards of various designs. The procedures for issuing an electronic payment card will be described in detail later.

[1390] The transaction list 5006 includes four types of information for one payment card issuance: a transaction number 5023, a service code 5024, a transaction time 5025, and a transaction information address 5026.

[1391] The transaction number 5023 uniquely represents the payment card issuance process; the service code 5024 represents the type of service provided by the payment card issuing system; the transaction time 5025 represents the time at which the payment card issuance process was performed; and the transaction information address 5026 is an address in the payment card issuer information server 906 at which is stored a receipt that was issued by the payment card issuing system 108.

[1392] The usage report list 5007 is management information for the usage report that the service providing system 110 issued to the payment card issuing system 108, and comprises a list of the usage report addresses 5027 that are located in the payment card issuer information server 906 in which the usage reports 5704 are stored.

[1393] The information stored in the telephone card issuer information server 907 of the service providing system 110 will now be explained.

[1394] The telephone card issuer information server 907 manages the attribute information for the telephone card issuer and the telephone card issuing history information. Fig. 51 is a specific diagram showing information stored in the telephone card issuer information server 907 for each telephone card issuer.

[1395] The telephone card issuer information server 907 stores eight types of information for each telephone card issuer: telephone card issuer data management information 5100, telephone card issuer information 5101, a telephone card issuer public key certificate 5102, a service code list 5103, an installation card list 5104, an electronic telephone card template list 5105, a transaction list 5106, and a usage report list 5107.

[1396] The telephone card issuer data management information 5100 is management information for data for each telephone card issuer that is to be stored in the telephone card issuer information server 907; the telephone card issuer information 5101 is information concerning a telephone card issuer, such as an address, an account number and the terms of a contract; the payment card issuer public key certificate 5102 is a certificate for the public key belonging to a telephone card issuer; the service code list 5103 is a list of service codes indicating the type of service provided by a telephone card issuer; the installation card list 5104 is list information for the installation card numbers of electronic telephone card installation cards issued by a telephone card issuer; the electronic telephone card template list 5105 is management information for a template program for an electronic telephone card that corresponds to a telephone card issued by a telephone card issuer; the transaction list 5106 is telephone card issuing history information for a telephone card issuer; and the usage report list 5107 is management information for a usage report that the service providing system 110 issued the telephone card issuing system 109.

[1397] The telephone card issuer data management information 5100 consists of ten types of information: a telephone card issuer processor name 5108, a telephone card issuer ID 5109, a telephone card issuer status 5110, a telephone card issuer information address 5111, a telephone card issuer public key certificate address 5112, a service code list address 5113, an installation card list address 5114, an electronic telephone card template list address 5115, a transaction list address 5116 and a usage report list address 5117.

[1398] The telephone card issuer status 5110 specifies the service status in the issuance process of the telephone card issuing system 107. The telephone card issuer information address 5111, the telephone card issuer public key certificate address 5112, the service code list address 5113, the installation card list address 5114, the electronic telephone card template list address 5115, the transaction list address 5116 and the usage report list address 5117 represent addresses in the telephone card issuer information server 907 at which respectively are stored the telephone card issuer information 5101, the telephone card issuer public key certificate 5102, the service code list 5103, the installation card list 5104, the electronic telephone card template list 5105, the transaction list 5106 or the usage report list 5107.

[1399] The electronic telephone card template program is a model for an electronic telephone card issued by the service providing system, and is registered in advance in the telephone card issuer information server 907 in accordance with the contract entered into by the telephone card issuer and the service provider. To issue an electronic telephone card, the service providing system employs the template program designated by the telephone card issuing system to generate an electronic telephone card, and transmits the telephone card to the mobile user terminal.

[1400] The electronic template list 5105 includes five information items for one type of electronic telephone card template program: a template code 5118, a transaction module address 5119, a representation module address 5120, a default representative component address 5121, and a telephone card clearing module address 5122.

[1401] The template code 5118 is code information describing the type of electronic telephone card template program. The transaction module address 5119 is an address in the telephone card issuer information server 907 at which is stored a program module that is the transaction module 2030 for an electronic telephone card that is generated. The representation module address 5120 is an address in the telephone card issuer information server 907 at which is stored a program module that is the representation module 2031 for an electronic telephone card that is generated. The default representative component address 5121 is an address in the telephone card issuer information server 907 at which default information is stored. The telephone card clearing module address 5122 is an address in the telephone card issuer information server 907 at which is stored a telephone card clearing module for clearing an electronic telephone card that is generated. And the telephone card clearing module is a program module that corresponds to the transaction module.

[1402] The electronic telephone card issuing commission 6203, which is a message by which the telephone card issuing system requests that the service providing system request the issuance of an electronic telephone card, includes not only telephone card information, such as the face value of the telephone card that is issued and the usage condition, but also a template code that specifies a template program and representative component information. The service providing system generates an electronic telephone card using the transaction module and the representation module specified by the template code, and the representative component information that is included in the electronic telephone card issuing commission.

[1403] Before the template program is registered in the telephone card issuer information server 907, the operation and the safety of the mobile electronic commerce system are confirmed. Since several template programs are stored in advance, the telephone card issuer can safely issue a telephone card that performs various operations, as well as telephone cards of various designs. The procedures for issuing an electronic telephone card will be described in detail later.

[1404] The transaction list 5106 includes four types of information for one telephone card issuance: a transaction number 5123, a service code 5124, a transaction time 5125, and a transaction information address 5126.

[1405] The transaction number 5123 uniquely represents the telephone card issuance process; the service code 5124 represents the type of service provided by the telephone card issuing system; the transaction time 5125 represents the time at which the telephone card issuance process was performed; and the transaction information address 5126 is an address in the telephone card issuer information server 907 at which is stored a receipt that was issued by the telephone card issuing system 109.

[1406] The usage report list 5107 is management information for the usage report that the service providing system 110 issued to the telephone card issuing system 109, and comprises a list of the usage report addresses 5127 that are located in the telephone card issuer information server 907 in which the usage

reports 5704 are stored.

[1407] The information stored in the service director information server 901 in the service providing system 110 will now be explained.

[1408] The service director information server 901 stores ten types of information: a user list 5200, a merchant list 5201, a transaction processors list 5202, a ticket issuers list 5203, a payment card issuers list 5204, a telephone card issuers list 5205, a provided service list 5206, electronic ticket management information 5300, electronic payment card management information 5400, and electronic telephone card management information 5500.

[1409] Figs. 52A to 52G are specific diagrams showing the user list 5200, the merchant list 5201, the transaction processors list 5202, the ticket issuers list 5203, the payment card issuers list 5204, the telephone card issuers list 5205 and the provided service list 5206, all of which are in the service director information server 901. Figs. 53 to 55 are specific diagrams respectively showing the electronic ticket management information 5300 stored for one type of electronic ticket, the electronic payment card management information 5400 stored for one type of electronic payment card, and the electronic telephone card management information 5500 stored for one type of electronic telephone card.

[1410] The user list 5200 is a list of attribute information for the mobile user terminals that have entered into contracts with a service provider; the merchant list 5201 is a list of attribution information for the gate terminals, the merchant terminals (102 or 103), the automatic vending machines (accounting machines) and the switching centers (electronic telephone card accounting machines) that have entered into contracts with the service provider; the transaction processors list 5202 is a list of the attribution information for all the transaction processors that have entered into contracts with the service provider; the ticket issuers list 5203 is a list of attribution information for all the ticket issuers who have entered into contracts with the service provider; the payment card issuers list 5204 is a list of attribution information for all the payment card issuers who have entered into contracts with the service provider; the telephone card issuers list 5205 is a list of attribution information for all the telephone card issuers who have entered into contracts with the service provider; the provided service list 5203 is a list of information for mobile electronic commerce service that has been provided by the service providing system 110; the electronic ticket management information 5300 is management information for a registered electronic ticket; the electronic payment card management information 5400 is management information for a registered electronic payment card; and the electronic telephone card management information 5500 is management information for a registered electronic telephone card.

[1411] In the user list 5200, six types of information are stored for each mobile user terminal: a user name 5207, a user ID 5208, a user telephone number 5209, a user public key certificate address 5210, an available service list address 5211, and a user information address 5212.

[1412] The user public key certificate address 5210 is an address at which a certificate for the public key of a user is stored; the available service list address 5211 is an address at which a list of service codes that the user can employ is stored; and the user information address 5212 is an address at which the user data management information 4600 for the pertinent user is stored.

[1413] In the merchant list 5201, seven types of information are stored for each gate terminal, each merchant terminal (102, 103), each automatic vending machine (accounting machine) or each switching center (electronic telephone card accounting machine): a merchant name (communication service provider name) 5213, a merchant ID (communication service provider ID) 5214, an accounting machine ID (gate ID) 5215, a merchant telephone number 5216, an available service list address 5217, a customers table address 5218, and a merchant information address 5219.

[1414] The available service list address 5217 is an address at which is stored a list of the service codes that the merchant or the service communication provider can handle. The customers table address 5218 is the address at which is stored table information (a customer table) that represents the correspondence credited to the customer number and the user ID. And the merchant information address 5219 is an address at which the merchant data management information 4700 for the pertinent merchant is stored.

[1415] In the transaction processors list 5202 five types of information are stored for each transaction processor: a transaction processor name 5220, a transaction processor ID 5221, a transaction processor communication ID 5222, an available service list address 5223, and a transaction processor information

address 5224.

[1416] The transaction processor communication ID 5222 is an ID for the transaction processing system 106 used when the service providing system 110 communicates with the transaction processing system 106 via the digital communication line 131. The available service list address 5223 is an address at which is stored a list of service codes that the transaction processor can handle. And the transaction processor information address 5224 is an address in the transaction processor information server 904 at which is stored the transaction processor data management information 4800 for the pertinent transaction processor.

[1417] In the ticket issuers list 5203 seven types of information are stored for each ticket issuer: a ticket issuer name 5225, a ticket issuer ID 5226, a ticket issuer communication ID 5227, an available service list address 5228, an installation card list address 5229, a customers table address 5230, and a ticket issuer information address 5231.

[1418] The ticket issuer communication ID 5227 is an ID for the ticket issuing system 107 used when the service providing system 110 communicates with the ticket issuing system 107 via the digital communication line 132. The available service list address 5228 is an address at which is stored a list of service codes that the ticket issuer can handle. The installation card list address 5229 is an address in the service director information server 901 at which is stored a list of installation card numbers for electronic ticket installation cards that are issued by the ticket issuer. The customer table address 5230 is an address in the service director information server 901 at which is stored table information (a customer table) that represents the correspondence credited to the customer number and the user ID. And the ticket issuer information address 5231 is an address in the ticket issuer information server 905 at which is stored the ticket issuer data management information 4900 for the pertinent ticket issuer.

[1419] In the payment card issuers list 5204 seven types of information are stored for each payment card issuer: a payment card issuer name 5232, a payment card issuer ID 5233, a payment card issuer communication ID 5234, an available service list address 5235, an installation card list address 5236, a customers table address 5237, and a payment card issuer information address 5238.

[1420] The payment card issuer communication ID 5234 is an ID for the payment card issuing system 108 used when the service providing system 110 communicates with the payment card issuing system 108 via the digital communication line 133. The available service list address 5235 is an address at which is stored a list of service codes that the payment card issuer can handle. The installation card list address 5236 is an address in the service director information server 901 at which is stored a list of installation card numbers for electronic payment card installation cards that are issued by the payment card issuer. The customer table address 5237 is an address in the service director information server 901 at which is stored table information (customer table) that represents the correspondence credited to the customer number and the user ID. And the payment card issuer information address 5238 is an address in the payment card issuer information server 906 at which is stored the payment card issuer data management information 5000 for the pertinent payment card issuer.

[1421] In the telephone card issuers list 5205 seven types of information are stored for each telephone card issuer: a telephone card issuer name 5239, a telephone card issuer ID 5240, a telephone card issuer communication ID 5241, an available service list address 5242, an installation card list address 5243, a customers table address 5244, and a telephone card issuer information address 5245.

[1422] The telephone card issuer communication ID 5241 is an ID for the telephone card issuing system 109 used when the service providing system 110 communicates with the telephone card issuing system 109 via the digital communication line 134. The available service list address 5242 is an address at which is stored a list of service codes that the telephone card issuer can handle. The installation card list address 5243 is an address in the service director information server 901 at which is stored a list of installation card numbers for electronic telephone card installation cards that are issued by the telephone card issuer. The customer table address 5244 is an address in the service director information server 901 at which is stored table information (a customer table) that represents the correspondence credited to the customer number and the user ID. And the telephone card issuer information address 5246 is an address in the telephone card issuer information server 907 at which is stored the telephone card issuer data management information 5100 for the pertinent telephone card issuer.

[1423] In the provided service list 5206 four types of information are stored for each occasion on which the

mobile electronic commerce service was provided: a service providing number 5246, a service code 5247, a service providing time 5248, and a provided service information address 5249.

[1424] The service providing number 5246 uniquely represents the process performed by the service providing system 110 on an occasion when service was provided. The service code 5247 is code information indicating the type of service provided. The service providing time 5248 is the time at which the mobile electronic commerce service was provided. And the provided service information address 5249 is an address in the service director information server 901 at which is stored history information for the processes performed by the service providing system 110 on an occasion when service was provided.

[1425] The electronic ticket management information 5300 is management information that is stored in the service director information server 901 for one type of electronic ticket.

[1426] In Fig. 53, 13 types of information are stored in the electronic ticket management information 5300: a ticket name 5304, a ticket code 5305, a ticket issuer ID 5306, a validity term 5307, a ticket private key 5308, a ticket public key 5309, a gate private key 5310, a gate public key 5311, a template code 5312, a management term 5313, a user list address 5314, a merchant list address 5315, and a registered ticket list address 5316.

[1427] The ticket name 5304 is information providing the name of an electronic ticket, the ticket code 5305 is code information describing the type of electronic ticket, the ticket issuer ID 5306 is ID information for a ticket issuer, and the validity term 5307 is the period during which an electronic ticket is valid. The ticket private key 5308 and the ticket public key 5309 are a pair of keys that are employed to authorize an electronic ticket in the ticket examination process, and the gate private key 5310 and the gate public key 5311 are a pair of keys that are employed to authorize a gate terminal in the ticket examination process. The service providing system employs the ticket private key 5308 and the gate public key 5311 to issue an electronic ticket, and employs the ticket public key 5309 and the gate private key 5310 to set up an electronic ticket for examination at the gate terminal.

[1428] The template code 5312 is code information that describes an electronic ticket template program and is used to generate an electronic ticket. The management term 5313 is a period during which the electronic ticket management information 5300 is managed by the service director information server 901. That is, when the management term 5313 expires, information in the electronic ticket management information 5300 is shifted to a management form or a storage medium for which a lower cost is assessed.

[1429] The user list address 5314 is an address in the service director information server 901 at which is stored the user list 5301 for a user who owns the pertinent electronic ticket. And the user list 5301 is list information in which two information entries, a ticket ID 5317 and a user ID 5318 identifying the owner of the ticket, are made for one electronic ticket.

[1430] The merchant list address 5315 is an address in the service director information server 901 at which is stored the merchant list 5302 identifying a merchant who is permitted to examine the electronic ticket. And the merchant list 5302 is list information for the merchant ID 5319 assigned to a merchant who is permitted to examine the electronic ticket.

[1431] When the contents of a ticket are to be modified, the user list 5301 and the merchant list 5302 are referred to in order to specify the owner of the ticket or the merchant who has set up the ticket examination module.

[1432] The registered ticket list address 5316 is an address in the service director information server 901 at which the registered ticket list 5303 for registered electronic tickets is stored. The registered ticket list 5303 is list information, for electronic tickets that have been registered, in which are stored seven types of information: a ticket ID 5320, an initial ticket examination number 5321, a user ID 5322, a user public key 5323, a registered ticket certificate address 5324, a ticket examination response list address 5325, and a former user information address 5326.

[1433] The user ID 5321 and the user public key 5323 are an ID and a public key for a user (the owner of an electronic ticket) who has registered an electronic ticket (the ticket ID 5320). The initial ticket examination number 5321 is the initial value of the ticket examination number for an electronic ticket. And the registered ticket certificate address 5324 is an address in the service director information server 901 at which a registered ticket certificate for an electronic ticket is stored.

[1434] The initial ticket examination number 5321 is an arbitrary number that the service providing system sets before issuing an electronic ticket. The ticket examination number is incremented each time the ticket examination process is performed. In the ticket reference process, the service providing system employs the ticket examination number to examine the ticket status 11103 and the variable ticket information 11104 that have been modified to determine whether they match.

[1435] In the ticket reference process, first, the service providing system examines the registered ticket list 5303 to determine whether the electronic ticket has been registered. Then, the service providing system employs the user public key 5323 to examine the user digital signature in the ticket examination response 6703, and employs the registered ticket certificate to examine the ticket digital signature in the ticket examination response 6703. Further, the service providing system employs the ticket examination number to examine the ticket status 11103 and the variable ticket information 11104 that have been modified to determine whether they match.

[1436] The ticket examination response list address 5325 is an address in the service director information server 901 at which is stored list information for a ticket examination response (a ticket examination response that is uploaded to the service providing system in the ticket reference process).

[1437] The former user information address 5326 is an address in the service director information server 901 at which is stored former user information 5327 concerning a preceding owner (user) of the electronic ticket. When an electronic ticket that is registered is transferred to another user, the service providing system updates the registered ticket list 5303 to reflect the new user information, and the old user information is managed as the former user information 5327.

[1438] The former user information 5327 consists of five types of information: a user ID 5328, a user public key 5329, a registered ticket certificate address 5330, a ticket examination response list address 5331, and a former user information address 5332. These addresses correspond respectively to the user ID 5322, the user public key 5323, the registered ticket certificate address 5324, the ticket examination response list address 5325 and the former user information address 5326, all of which are in the registered ticket list. In addition, when another owner preceded the present owner, the former user information address 5332 is an address of the former user information for the pertinent owner.

[1439] That is, when the electronic ticket that is registered is transferred, the user ID 5322, the user public key 5323, the registered ticket certificate address 5324, the ticket examination response list address 5325 and the former user information address 5326 are updated, and at the former user information address 5326, the information stored in those portions before the updating is pointed to as the former user information 5327

[1440] Since the electronic ticket is managed in the above described manner, the usage condition of the electronic ticket can be precisely understood even when it is transferred.

[1441] The electronic payment management information 5400 is management information that is stored in the service director information server 901 for one type of electronic payment card.

[1442] In Fig. 54, 12 types of information are stored in the electronic payment card management information 5400: a card name 5403, a card code 5404, a payment card issuer ID 5405, a validity term 5406, a card private key 5407, a card public key 5408, an accounting machine private key 5409, an accounting machine public key 5410, a template code 5411, a management term 5412, a merchant list address 5413, and a registered card list address 5414.

[1443] The card name 5403 is information providing the name of an electronic payment card, the card code 5404 is code information describing the type of electronic payment card, the payment card issuer ID 5405 is ID information for a payment card issuer, and the validity term 5406 is the period during which an electronic payment card is valid. The card private key 5407 and the card public key 5408 are a pair of keys that are employed to authorize an electronic payment card in the payment card clearing process, and the accounting machine private key 5409 and the accounting machine public key 5410 are a pair of keys that are employed to authorize the merchant terminal 102 or 103 or the automatic vending machine 104 in the payment card clearing process. The service providing system employs the card private key 5407 and the accounting machine public key 5410 to issue an electronic payment card, and employs the card public key 5408 and the accounting machine private key 5409 to set up an electronic payment card that a merchant

handles at the merchant terminal 102 or 103 or the automatic vending machine 104.

[1444] The template code 5411 is code information that describes an electronic payment card template program and is used to generate an electronic payment card. The management term 5412 is a period during which the electronic payment card management information 5400 is managed by the service director information server 901. That is, when the management term 5412 expires, information in the electronic payment card management information 5400 is shifted to a management form or a storage medium for which a lower cost is assessed.

[1445] The merchant list address 5413 is an address in the service director information server 901 at which is stored the merchant list 5401 identifying a merchant who is permitted to use the electronic payment card. And the merchant list 5401 is list information for the merchant ID 5415 assigned to a merchant who is permitted to handle the electronic payment card.

[1446] The registered card list address 5414 is an address in the service director information server 901 at which the registered card list 5402 for registered electronic payment cards is stored. The registered card list 5402 is list information, for electronic payment cards that have been registered, in which are stored seven types of information: a card ID 5416, an initial micro-check issuing number 5417, a user ID 5418, a user public key 5419, a registered card certificate address 5420, a micro-check list address 5421, and a former user information address 5422.

[1447] The user ID 5418 and the user public key 5419 are an ID and a public key for a user (the owner of an electronic payment card) who has registered an electronic payment card (the card ID 5416). The initial micro-check issuing number 5417 is the initial value of the micro-check issuing number for an electronic payment card. And the registered card certificate address 5420 is an address in the service director information server 901 at which a registered card certificate for an electronic payment card is stored.

[1448] The initial micro-check issuing number 5417 is an arbitrary number that the service providing system sets before issuing an electronic payment card. The micro-check issuing number is incremented each time the payment card clearing process is performed (each time the micro-check is issued). In the payment card reference process, the service providing system employs the micro-check issuing number to examine the amount of payment 11303, the card status 11304 and the total remaining value 11305 that have been modified to determine whether they match.

[1449] In the payment card reference process, first, the service providing system examines the registered card list 5402 to determine whether the electronic payment card has been registered. Then, the service providing system employs the user public key 5419 to examine the user digital signature in the micro-check, and employs the registered card certificate to examine the card digital signature in the micro-check. Further, the service providing system employs the micro-check issuing number to examine the amount of payment 11303, the card status 11304 and the total remaining value 11305 that have been modified to determine whether they match.

[1450] The micro-check list address 5421 is an address in the service director information server 901 at which is stored list information for a micro-check (a micro-check that is uploaded to the service providing system in the payment card reference process).

[1451] The former user information address 5422 is an address in the service director information server 901 at which is stored former user information 5423 concerning a preceding owner (user) of the electronic payment card. When an electronic payment card that is registered is transferred to another user, the service providing system updates the registered card list 5402 to reflect the new user information, and the old user information is managed as the former user information 5423.

[1452] The former user information 5423 consists of five types of information: a user ID 5424, a user public key 5425, a registered card certificate address 5426, a micro-check list address 5427, and a former user information address 5428. These addresses correspond respectively to the user ID 5418, the user public key 5419, the registered card certificate address 5420, the micro-check list address 5421 and the former user information address 5422, all of which are in the registered card list. In addition, when another owner preceded the present owner, the former user information address 5428 is an address of the former user information for the pertinent owner.

[1453] That is, when the electronic payment card that is registered is transferred, the user ID 5418, the user

public key 5419, the registered card certificate address 5420, the micro-check list address 5421, and the former user information address 5422 are updated, and at the former user information address 5422, the information stored in those portions before the updating is pointed to as the former user information 5423.

[1454] Since the electronic payment card is managed in the above described manner, the usage condition of the electronic payment card can be precisely understood even when it is transferred. Thus, even when the transfer of an electronic payment card that is partially used is permitted, the safety of the system is not deteriorated.

[1455] The electronic telephone management information 5500 is management information that is stored in the service director information server 901 for one type of electronic telephone card.

[1456] In Fig. 55, 12 types of information are stored in the electronic telephone card management information 5500: a card name 5503, a card code 5504, a telephone card issuer ID 5505, a validity term 5506, a card private key 5507, a card public key 5508, an accounting machine private key 5509, an accounting machine public key 5510, a template code 5511, a management term 5512, a communication service provider list address 5513, and a registered card list address 5514.

[1457] The card name 5503 is information providing the name of an electronic telephone card, the card code 5504 is code information describing the type of electronic telephone card, the telephone card issuer ID 5505 is ID information for a telephone card issuer, and the validity term 5506 is the period during which an electronic telephone card is valid. The card private key 5507 and the card public key 5508 are a pair of keys that are employed to authorize an electronic telephone card in the telephone card clearing process, and the accounting machine private key 5509 and the accounting machine public key 5510 are a pair of keys that are employed to authorize the electronic telephone card accounting machine 800 in the telephone card clearing process. The service providing system employs the card private key 5507 and the accounting machine public key 5510 to issue an electronic telephone card, and employs the card public key 5508 and the accounting machine private key 5509 to set up an electronic telephone card that a communication service provider handles at the electronic telephone card accounting machine 800.

[1458] The template code 5511 is code information that describes an electronic telephone card template program and is used to generate an electronic telephone card. The management term 5512 is a period during which the electronic telephone card management information 5500 is managed by the service director information server 901. That is, when the management term 5512 expires, information in the electronic telephone card management information 5500 is shifted to a management form or a storage medium for which a lower cost is assessed.

[1459] The communication service provider list address 5513 is an address in the service director information server 901 at which is stored the communication service provider list 5501 identifying a communication service provider who is permitted to handle the electronic telephone card. And the communication service provider list 5501 is list information for the communication service provider ID 5515 assigned to a communication service provider who is permitted to handle the electronic telephone card.

[1460] The registered card list address 5514 is an address in the service director information server 901 at which the registered card list 5502 for registered electronic telephone cards is stored. The registered card list 5502 is list information, for electronic telephone cards that have been registered, in which are stored seven types of information: a card ID 5516, an initial micro-check issuing number 5517, a user ID 5518, a user public key 5519, a registered card certificate address 5520, a telephone micro-check list address 5521, and a former user information address 5522.

[1461] The user ID 5518 and the user public key 5519 are an ID and a public key for a user (the owner of an electronic telephone card) who has registered an electronic telephone card (the card ID 5516). The initial micro-check issuing number 5517 is the initial value of the micro-check issuing number for an electronic telephone card. And the registered card certificate address 5520 is an address in the service director information server 901 at which a registered card certificate for an electronic telephone card is stored.

[1462] The initial micro-check issuing number 5517 is an arbitrary number that the service providing system sets before issuing an electronic telephone card. The micro-check issuing number is incremented each time the telephone card clearing process is performed (each time the telephone micro-check is issued). In the telephone card reference process, the service providing system employs the micro-check issuing number to